Cisco ASR 5000 Series Command Line Interface Reference
Version 10.0

Last Updated June 30, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22948-01
radius accounting apn-to-be-included .......................................................... 121
radius accounting algorithm ................................................................. 122
radius accounting billing-version .......................................................... 124
radius accounting gtp trigger-policy ......................................................... 125
radius accounting ha policy ................................................................. 126
radius accounting interim ................................................................. 127
radius accounting ip remote-address ....................................................... 129
radius accounting keepalive ............................................................... 130
radius accounting pdif trigger-policy ...................................................... 132
radius accounting rp ................................................................. 133
radius accounting server ................................................................. 136
radius algorithm ................................................................. 139
radius allow ................................................................. 140
radius attribute ................................................................. 141
radius authenticate ............................................................... 144
radius authenticator-validation ............................................................ 146
radius charging ................................................................. 147
radius charging accounting algorithm ................................................. 149
radius charging accounting server ....................................................... 150
radius charging algorithm ............................................................... 152
radius charging server ................................................................. 153
radius ip vrf ........................................................................ 155
radius keepalive ........................................................................ 156
radius mediation-device .................................................................. 158
radius probe-interval ..................................................................... 159
radius probe-max-retries ................................................................. 160
radius probe-timeout ..................................................................... 161
radius server ........................................................................... 162

AAL2 Node Configuration Mode Commands ............................................. 165
aal2-path-id ........................................................................ 166
end ...................................................................................... 168
exit ...................................................................................... 169
point-code ........................................................................ 170

Accounting Policy Configuration Mode Commands ............................ 171
accounting-event-trigger ................................................................. 172
accounting-level ..................................................................... 174
accounting-mode ..................................................................... 176
cc profile ........................................................................ 177
end ...................................................................................... 179
exit ...................................................................................... 180
operator-string ........................................................................ 181

ACL Configuration Mode Commands ............................................... 183
deny/permit ........................................................................ 184
deny/permit (by source IP address masking) ..................................... 185
deny/permit (any) .................................................................... 187
deny/permit (by host IP address) .................................................... 189
deny/permit (by source ICMP packets) ............................................ 191
deny/permit (by IP packets) ............................................................ 194
deny/permit (by TCP/UDP packets) .................................................... 197
end ...................................................................................... 201
exit ...................................................................................... 202
readaddr server ........................................................................ 203
redirect context ........................................................................ 207
redirect context (by IP address masking) ............................................. 208
ALCAP Configuration Mode Commands

- aal2-node
- aal2-route
- associate
- end
- exit
- maximum reset-retransmission
- self-point-code
- timeout alcap
- timeout stc

APN Configuration Mode Commands

- aaa group
- access-link
- accounting-mode
- active-charging bandwidth-policy
- active-charging rulebase
- apn-ambr
- associate accounting-policy
- authentication
- bearer-control-mode
- cc-home
- cc-roaming
- cc-sgsn
- cc-visiting
- content-filtering category
- credit-control-group
- data-tunneling ignore df-bit
- data-tunnel mtu
- dcca origin endpoint
- dcca peer-select
- default
- dhcp context-name
- dhcp lease-expiration-policy
- dhcp service-name
- dns
- ehrpd-access
- end
- exit
- firewall policy
- fw-and-nat policy
- gsm-qos negotiate
- gtpp group
- gtpp secondary-group
- idle-timeout-activity ignore-downlink
- ims-auth-service
- ip access-group
- ip address alloc-method
- ip address pool
- ip context-name
- ip header-compression
- ip hide-service-address
- ip local-address
- ip multicast discard
- ip qos-dscp

xheader-format

ALCAP Configuration Mode Commands

- aal2-node
- aal2-route
- associate
- end
- exit
- maximum reset-retransmission
- self-point-code
- timeout alcap
- timeout stc

APN Configuration Mode Commands

- aaa group
- access-link
- accounting-mode
- active-charging bandwidth-policy
- active-charging rulebase
- apn-ambr
- associate accounting-policy
- authentication
- bearer-control-mode
- cc-home
- cc-roaming
- cc-sgsn
- cc-visiting
- content-filtering category
- credit-control-group
- data-tunneling ignore df-bit
- data-tunnel mtu
- dcca origin endpoint
- dcca peer-select
- default
- dhcp context-name
- dhcp lease-expiration-policy
- dhcp service-name
- dns
- ehrpd-access
- end
- exit
- firewall policy
- fw-and-nat policy
- gsm-qos negotiate
- gtpp group
- gtpp secondary-group
- idle-timeout-activity ignore-downlink
- ims-auth-service
- ip access-group
- ip address alloc-method
- ip address pool
- ip context-name
- ip header-compression
- ip hide-service-address
- ip local-address
- ip multicast discard
- ip qos-dscp

xheader-format

ALCAP Configuration Mode Commands

- aal2-node
- aal2-route
- associate
- end
- exit
- maximum reset-retransmission
- self-point-code
- timeout alcap
- timeout stc

APN Configuration Mode Commands

- aaa group
- access-link
- accounting-mode
- active-charging bandwidth-policy
- active-charging rulebase
- apn-ambr
- associate accounting-policy
- authentication
- bearer-control-mode
- cc-home
- cc-roaming
- cc-sgsn
- cc-visiting
- content-filtering category
- credit-control-group
- data-tunneling ignore df-bit
- data-tunnel mtu
- dcca origin endpoint
- dcca peer-select
- default
- dhcp context-name
- dhcp lease-expiration-policy
- dhcp service-name
- dns
- ehrpd-access
- end
- exit
- firewall policy
- fw-and-nat policy
- gsm-qos negotiate
- gtpp group
- gtpp secondary-group
- idle-timeout-activity ignore-downlink
- ims-auth-service
- ip access-group
- ip address alloc-method
- ip address pool
- ip context-name
- ip header-compression
- ip hide-service-address
- ip local-address
- ip multicast discard
- ip qos-dscp
authentication ................................................................................................................ 551
bind ............................................................................................................................... 552
bs-monitor .................................................................................................................. 553
end ............................................................................................................................... 555
exit ............................................................................................................................... 556
gre ............................................................................................................................... 557
handover ...................................................................................................................... 558
idle-mode .................................................................................................................... 560
max-retransmission ..................................................................................................... 562
mobile-ip ..................................................................................................................... 563
peer-asngw ............................................................................................................... 564
policy .......................................................................................................................... 565
policy asngw-initiated-reauth .................................................................................... 567
policy overload .......................................................................................................... 569
ran-peer-map ............................................................................................................ 570
retransmission-timeout ............................................................................................. 571
secondary-ip-hosts .................................................................................................... 572
setup-timeout ............................................................................................................. 573

ASN Paging Controller Configuration Mode Commands ................................. 575
ASN Paging Group Configuration Mode Commands .............................................. 589
ASN QoS Descriptor Configuration Mode Commands ........................................ 595
ASN RAN Peer Map Configuration Mode Commands ........................................ 603
ASN Service Profile Configuration Mode Commands .......................................... 607
ATM Port Configuration Mode Commands ........................................ 615
  default......................................................................................... 616
  description.................................................................................... 617
  end................................................................................................. 618
  exit................................................................................................. 619
  line-timing..................................................................................... 620
  preferred slot ............................................................................... 621
  pvc............................................................................................... 622
  shutdown......................................................................................... 623
  snmp trap link-status...................................................................... 624
  threshold high-activity..................................................................... 625
  threshold monitoring......................................................................... 627
  threshold rx-utilization..................................................................... 629
  threshold tx-utilization..................................................................... 631

Bandwidth Policy Configuration Mode Commands ....................... 633
  end................................................................................................. 634
  exit................................................................................................. 635
  flow limit-for-bandwidth.................................................................. 636
  group-id......................................................................................... 637

BGP Address-Family (IPv4/IPv6) Configuration Mode Commands...... 639
  end................................................................................................. 641
  exit................................................................................................. 642
  neighbor......................................................................................... 643
  network......................................................................................... 646
  redistribute.................................................................................. 647

BGP Address-Family (VPNv4) Configuration Mode Commands ....... 649
  end................................................................................................. 651
  exit................................................................................................. 652
  neighbor......................................................................................... 653

BGP Address-Family (VPNv4) Configuration Mode Commands ....... 655
  end................................................................................................. 657
  exit................................................................................................. 658
  neighbor......................................................................................... 659
  redistribute.................................................................................. 662

BITS Port Configuration Mode Commands .................................. 665
  default......................................................................................... 666
  description...................................................................................... 667
  end................................................................................................. 668
  exit................................................................................................. 669
  mode.............................................................................................. 670
  preferred slot................................................................................ 671
  recover.......................................................................................... 672
  shutdown....................................................................................... 673
  snmp trap link-status...................................................................... 674

BMSC Profile Configuration Mode Commands ............................. 675
  end................................................................................................. 676
  exit................................................................................................. 677
  gmb diameter dictionary ............................................................... 678
  gmb diameter endpoint................................................................. 679
  gmb diameter peer-select............................................................ 680
  gmb user-data................................................................................ 682
Border Gateway Protocol Configuration Mode Commands .................. 685
    address-family ipv4 .......................................................................... 686
    address-family ipv6 .......................................................................... 688
    address-family vpnv4 ....................................................................... 689
    distance ............................................................................................. 690
    end ..................................................................................................... 692
    enforce-first-as .................................................................................. 693
    exit ..................................................................................................... 694
    ip vrf .................................................................................................. 695
    neighbor ............................................................................................ 696
    network .............................................................................................. 699
    redistribute ........................................................................................ 700
    router-id ........................................................................................... 701
    scan-time ........................................................................................... 702
    timers ................................................................................................. 703

Border Gateway Protocol IP VRF Configuration Mode Commands ....... 705
    end ..................................................................................................... 707
    exit ..................................................................................................... 708
    route-distinguisher ............................................................................. 709
    route-target ....................................................................................... 710

Bulk Statistics File Configuration Mode Commands .............................. 713

Bulk Statistics Configuration Mode Commands ...................................... 715
    Common Syntax Options .................................................................... 716
    Schema Format String Syntax ............................................................ 716
    Common Statistics ............................................................................ 717
    apn schema ......................................................................................... 718
    asngw schema ................................................................................... 719
    bcmcs schema .................................................................................... 721
    card schema ....................................................................................... 722
    context schema .................................................................................. 724
    cscf schema ....................................................................................... 726
    deca schema ....................................................................................... 728
    default ................................................................................................. 729
    dpca schema ....................................................................................... 730
    ecs schema .......................................................................................... 731
    egtpc schema ..................................................................................... 732
    end ..................................................................................................... 734
    exit ..................................................................................................... 735
    fa schema ........................................................................................... 736
    file ...................................................................................................... 737
    footer ................................................................................................. 739
    gather-on-standby .............................................................................. 741
    gprs schema ....................................................................................... 742
    gtpe schema ....................................................................................... 743
    gtpv schema ....................................................................................... 745
    ha schema ........................................................................................... 746
    header ................................................................................................. 747
    ippool schema .................................................................................... 749
    ipsg schema ....................................................................................... 750
    lae schema .......................................................................................... 751
    limit ..................................................................................................... 753
    lma schema ......................................................................................... 754
    local-directory .................................................................................. 756
### Card Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>mag schema</td>
<td>757</td>
</tr>
<tr>
<td>mipv6ha schema</td>
<td>758</td>
</tr>
<tr>
<td>nat-realm schema</td>
<td>759</td>
</tr>
<tr>
<td>pdef schema</td>
<td>760</td>
</tr>
<tr>
<td>port schema</td>
<td>761</td>
</tr>
<tr>
<td>ppp schema</td>
<td>762</td>
</tr>
<tr>
<td>radius schema</td>
<td>764</td>
</tr>
<tr>
<td>receiver</td>
<td>766</td>
</tr>
<tr>
<td>remotefile</td>
<td>768</td>
</tr>
<tr>
<td>rp schema</td>
<td>770</td>
</tr>
<tr>
<td>sample-interval</td>
<td>772</td>
</tr>
<tr>
<td>sccp schema</td>
<td>773</td>
</tr>
<tr>
<td>schema</td>
<td>774</td>
</tr>
<tr>
<td>sgsn schema</td>
<td>776</td>
</tr>
<tr>
<td>sgtp schema</td>
<td>777</td>
</tr>
<tr>
<td>ss7link schema</td>
<td>778</td>
</tr>
<tr>
<td>ss7rd schema</td>
<td>779</td>
</tr>
<tr>
<td>show variables</td>
<td>780</td>
</tr>
<tr>
<td>transfer-interval</td>
<td>781</td>
</tr>
</tbody>
</table>

### Channelized Port Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm-disable</td>
<td>802</td>
</tr>
<tr>
<td>alarm-soak-timer</td>
<td>803</td>
</tr>
<tr>
<td>clock-source</td>
<td>804</td>
</tr>
<tr>
<td>description</td>
<td>805</td>
</tr>
<tr>
<td>dlic</td>
<td>806</td>
</tr>
<tr>
<td>end</td>
<td>808</td>
</tr>
<tr>
<td>exit</td>
<td>809</td>
</tr>
<tr>
<td>frame-relay</td>
<td>810</td>
</tr>
<tr>
<td>hopath-sdsf</td>
<td>812</td>
</tr>
<tr>
<td>line-timing</td>
<td>813</td>
</tr>
<tr>
<td>loopback</td>
<td>814</td>
</tr>
<tr>
<td>lopath-sdsf</td>
<td>815</td>
</tr>
<tr>
<td>mtp2</td>
<td>816</td>
</tr>
<tr>
<td>path</td>
<td>817</td>
</tr>
<tr>
<td>preferred slot</td>
<td>821</td>
</tr>
<tr>
<td>pwe3-cesopsn</td>
<td>822</td>
</tr>
<tr>
<td>shutdown</td>
<td>823</td>
</tr>
<tr>
<td>snmp trap link-status</td>
<td>824</td>
</tr>
<tr>
<td>threshold high-activity</td>
<td>825</td>
</tr>
<tr>
<td>threshold monitoring</td>
<td>827</td>
</tr>
<tr>
<td>threshold rx-utilization</td>
<td>829</td>
</tr>
<tr>
<td>threshold tx-utilization</td>
<td>831</td>
</tr>
<tr>
<td>toh-sdsf</td>
<td>833</td>
</tr>
</tbody>
</table>
Charging Action Configuration Mode Commands

billing-action ............................................. 836
cca charging ............................................... 838
charge-units ............................................... 840
charge-volume ........................................... 841
content-filtering processing server-group ............ 844
content-id .................................................. 845
end ........................................................ 846
exit ......................................................... 847
flow action ................................................ 848
flow action redirect-url ................................ 850
flow idle-timeout ........................................ 853
flow limit-for-bandwidth ................................. 854
flow limit-for-flow-type ................................. 857
ip tos ...................................................... 858
ip vlan ...................................................... 860
nexthop-forwarding-address ......................... 861
qos-class-identifier ................................... 862
qos-renegotiate ......................................... 863
retransmissions-counted .................... 865
service-identifier ...................................... 866
tft packet-filter ........................................ 867
tos ........................................................ 868
xheader-insert ........................................... 870

Class-Map Configuration Mode Commands............... 873
end ........................................................ 874
exit ......................................................... 875
match any .................................................. 876
match dst-ip-address ................................... 877
match dst-port-range ................................... 878
match ip-tos ............................................ 879
match ipsec-spi ......................................... 880
match packet-size ........................................ 881
match protocol ........................................... 882
match src-ip-address .................................... 883
match src-port-range ................................... 884

Content Filtering Policy Configuration Mode Commands ........ 885
analyze ..................................................... 886
discarded-flow-content-id ....................... 889
failure-action ............................................ 890
timeout action ........................................... 892

Content Filtering Server Group Configuration Mode Commands .......... 893
connection retry-timeout ............................ 894
deny-message ........................................... 895
dictionary ................................................ 896
end ........................................................ 897
exit ......................................................... 898
failure-action ........................................... 899
icap server ................................................ 902
origin address .......................................... 904
response-timeout ....................................... 905
timeout action ........................................... 906
Context Configuration Mode Commands

aaa accounting .................................................................................. 910
aaa authentication ............................................................................. 912
aaa constructed-nai .......................................................................... 914
aaa filter-id rulebase mapping .......................................................... 917
aaa group .......................................................................................... 918
aaa nai-policy .................................................................................... 919
access-list undefined ......................................................................... 920
administrator ....................................................................................... 921
apn ...................................................................................................... 924
asn-qos-descriptor .............................................................................. 925
asn-service-profile ............................................................................ 927
asngw-service .................................................................................... 929
asnpc-service ..................................................................................... 931
bmse-profile ........................................................................................ 933
busyout ip pool ................................................................................... 934
class-map .......................................................................................... 936
closedrp-rp handoff ........................................................................... 938
cconfig-administrator ....................................................................... 939
content-filtering .................................................................................. 942
credit-control-service ....................................................................... 943
crypto group ........................................................................................ 944
crypto ipsec transform-set ................................................................ 945
crypto map .......................................................................................... 947
crypto node ........................................................................................ 949
crypto template ................................................................................... 950
cscf ...................................................................................................... 952
cscf acl ................................................................................................ 954
cscf ifc-filter-criteria ........................................................................ 955
cscf ifc-spt-condition ........................................................................ 957
cscf ifc-spt-group ............................................................................... 959
cscf ifc-trigger-point .......................................................................... 961
cscf isc-template ................................................................................ 963
cscf last-route-profile ...................................................................... 964
cscf peer-servers ............................................................................... 966
cscf policy ........................................................................................... 968
cscf routes .......................................................................................... 970
cscf service ........................................................................................ 971
cscf session-template .......................................................................... 973
cscf translation ................................................................................... 974
cscf urn-service-list .......................................................................... 975
css server ............................................................................................ 976
default aaa .......................................................................................... 977
default access-list ............................................................................... 978
default gtp ............................................................................................ 979
default mobile-ip ................................................................................. 982
default network-requested-pdp-context ............................................. 983
default ppp ............................................................................................ 984
default radius ........................................................................................ 987
default radius authenticate null-username ........................................ 990
default threshold .................................................................................. 991
dhcp-service ......................................................................................... 992
diameter accounting ........................................................................... 993
diameter authentication ................................................................. 996
  diameter authentication failure-handling .................................... 999
  diameter dictionary ................................................................. 1001
  diameter endpoint ................................................................. 1002
  diameter scip ................................................................. 1003
  diameter origin ................................................................. 1004
  dns-client ................................................................. 1005
  domain ................................................................. 1006
  eap-profile ................................................................. 1007
  cdn-module active-charging-service ......................................... 1008
  egtp-service ................................................................. 1009
  end ................................................................. 1011
  egress ................................................................. 1012
  external-inline-server .......................................................... 1013
  fa-service ................................................................. 1014
  firewall max-associations ..................................................... 1015
  ggsn-service ................................................................. 1016
  gprs-service ................................................................. 1017
  gs-service ................................................................. 1018
  gtp ................................................................. 1019
  gtp algorithm ................................................................. 1020
  gtp attribute ................................................................. 1021
  gtp charging-agent ........................................................... 1025
  gtp data-request sequence-numbers ........................................ 1027
  gtp dead-server suppress-cdrs ............................................... 1028
  gtp deadtime ................................................................. 1029
  gtp detect-dead-server ........................................................ 1030
  gtp dictionary ................................................................. 1031
  gtp duplicate-hold-time ....................................................... 1033
  gtp echo-interval ............................................................ 1034
  gtp egcdr ................................................................. 1036
  gtp error-response ............................................................ 1038
  gtp group ................................................................. 1039
  gtp max-cdrs ................................................................. 1040
  gtp max-pdu-size ............................................................. 1041
  gtp max-retries ............................................................... 1042
  gtp node-id ................................................................. 1043
  gtp redirection-allowed ...................................................... 1044
  gtp redirection-disallowed .................................................. 1045
  gtp server ................................................................. 1046
  gtp source-port-validation .................................................... 1048
  gtp storage-server ............................................................ 1049
  gtp storage-server local file .................................................. 1050
  gtp storage-server max-retries ............................................. 1052
  gtp storage-server mode ..................................................... 1053
  gtp storage-server timeout .................................................. 1054
  gtp suppress-cdrs zero-volume-and-duration ................................ 1055
  gtp timeout ................................................................. 1056
  gtp trigger ................................................................. 1057
  gtp transport-layer ........................................................... 1058
  gtpu-service ................................................................. 1059
  ha-service ................................................................. 1061
  hmbgw-service ............................................................... 1062
  hsgw-service ................................................................. 1064
  ikev1 disable-phase1-rekey ................................................... 1066
  ikev1 keepalive dpd .......................................................... 1067
ikev1 policy ................................................................. 1069
ikev2-ikesa ................................................................. 1070
ims-auth-service ......................................................... 1071
ims-sh-service ........................................................... 1072
inspector ................................................................. 1073
interface .................................................................. 1076
ip ................................................................................. 1078
ip access-group ......................................................... 1079
ip access-list ................................................................ 1081
ip arp ........................................................................ 1083
ip as-path access-list ................................................. 1085
ip dns-proxy source-address ........................................ 1086
ip domain-lookup ....................................................... 1087
ip domain-name .......................................................... 1088
ip forward .................................................................. 1089
ip identification packet-size-threshold ......................... 1090
ip localhost ............................................................... 1091
ip name-servers ........................................................ 1092
ip pool ....................................................................... 1093
ip prefix-list .............................................................. 1104
ip prefix-list sequence-number .................................. 1106
ip route ...................................................................... 1107
ip routing maximum-paths ......................................... 1110
ip routing overlap-pool ............................................. 1111
ip vrf ......................................................................... 1112
ipms ........................................................................ 1114
ipsec ......................................................................... 1115
ipsg-service .............................................................. 1116
ipv6 access-group ...................................................... 1118
ipv6 access-list ........................................................ 1119
ipv6 dns-proxy .......................................................... 1120
ipv6 neighbor ............................................................ 1121
ipv6 pool ................................................................ 1122
ipv6 route ................................................................. 1126
isakmp disable-phase1-rekey ....................................... 1128
isakmp keepalive ....................................................... 1129
isakmp policy ............................................................ 1130
iups-service ............................................................... 1131
l2tp peer-dead-time ...................................................... 1132
lac-service ................................................................. 1133
lma-service ............................................................... 1134
lns-service ................................................................. 1136
lawful-intercept ......................................................... 1137
lawful-intercept dictionary ........................................ 1140
mobile-ip ha reconnect ............................................. 1141
mag-service .................................................................. 1142
map-service ............................................................. 1144
mme-hss-service ........................................................ 1145
mme-service ............................................................. 1147
mobile-ip ................................................................. 1149
mobile-ip fa newcall .................................................. 1150
mobile-ip ha assignment-table .................................. 1151
mobile-ip ha newcall ................................................. 1152
mobile-ip ha reconnect ............................................. 1154
mpls bgp forwarding ................................................ 1155
nw-reachability server ............................................... 1156
Crypto Template Configuration Mode Commands ........................................ 1320
switchover ................................................................................................. 1321

Crypto Map Dynamic Configuration Mode Commands .............................. 1321
end ............................................................................................................. 1322
exit ............................................................................................................ 1323
set ............................................................................................................. 1324

Crypto Map IKEv1 Configuration Mode Commands ................................. 1327
end ............................................................................................................. 1328
exit ............................................................................................................ 1329
match address ............................................................................................ 1330
match crypto group .................................................................................... 1331
match ip pool .............................................................................................. 1332
set ............................................................................................................. 1333

Crypto Map IKEv2-IPv6 Configuration Mode Commands ........................ 1337
authentication ......................................................................................... 1338
certificate ................................................................................................. 1339
dns-handling .............................................................................................. 1340
exit ............................................................................................................. 1341
ikev2-ikesa ................................................................................................. 1342
match ........................................................................................................ 1344
payload ..................................................................................................... 1345
peer ............................................................................................................ 1346

Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands ......... 1347
end ............................................................................................................. 1349
exit ............................................................................................................ 1350
ipsec .......................................................................................................... 1351
lifetime ...................................................................................................... 1352
rekey .......................................................................................................... 1353

Crypto Map Manual Configuration Mode Commands .............................. 1355
end ............................................................................................................. 1356
exit ............................................................................................................ 1357
match address ............................................................................................ 1358
set control-dont-fragment ......................................................................... 1359
set peer ...................................................................................................... 1360
set session-key ......................................................................................... 1361
set transform-set ...................................................................................... 1363

Crypto Template Configuration Mode Commands .................................... 1365
authentication ......................................................................................... 1366
certificate ................................................................................................. 1368
default ....................................................................................................... 1369
dns-cookie ................................................................................................. 1370
dns-handling .............................................................................................. 1372
dos ........................................................................................................ 1374
end ............................................................................................................. 1376
exit ............................................................................................................ 1377
ikev2-ikesa ................................................................................................. 1378
keepalive ................................................................................................. 1380
nai .............................................................................................................. 1381
natt ............................................................................................................ 1382
payload ..................................................................................................... 1383
Crypto Template IKEv2-PDIF Payload Configuration Mode Commands 1385
  default.................................................................................................................. 1387
  end......................................................................................................................... 1389
  exit......................................................................................................................... 1390
  ignore-rekeying-requests....................................................................................... 1391
  ip-address-allocation............................................................................................. 1392
  ipsec ...................................................................................................................... 1393
  lifetime .................................................................................................................. 1394
  maximum-child-sa ............................................................................................... 1395
  rekey .................................................................................................................... 1396
  tsi .......................................................................................................................... 1397
  tsf .......................................................................................................................... 1398

Crypto Transform Set Configuration Mode Commands ......................... 1399
  end......................................................................................................................... 1400
  exit......................................................................................................................... 1401
  mode...................................................................................................................... 1402

CSCF Access Profile Configuration Mode Commands ...................... 1403
  access-security-type ............................................................................................. 1404
  authentication ....................................................................................................... 1405
  end......................................................................................................................... 1406
  exit......................................................................................................................... 1407
  sigcomp ................................................................................................................. 1408
  timeout................................................................................................................ 1409

CSCF ACL Configuration Mode Commands ........................................ 1411
  after....................................................................................................................... 1412
  before .................................................................................................................... 1413
  deny....................................................................................................................... 1414
  end......................................................................................................................... 1416
  exit......................................................................................................................... 1417
  permit................................................................................................................... 1418

CSCF Aor Policy Rules Configuration Mode Commands ................ 1421
  after....................................................................................................................... 1422
  aor ......................................................................................................................... 1423
  before .................................................................................................................... 1424
  end......................................................................................................................... 1425
  exit......................................................................................................................... 1426

CSCF Charging Configuration Mode Commands .............................. 1427
  end......................................................................................................................... 1428
  exclude............................................................................................................... 1429
  exit......................................................................................................................... 1431

CSCF Crypto Template Configuration Mode Commands .................. 1433
  end......................................................................................................................... 1434
  exit......................................................................................................................... 1435
  ipsec .................................................................................................................... 1436

CSCF Emergency-CSCF Configuration Mode Commands ............... 1437
  end......................................................................................................................... 1438
  exit......................................................................................................................... 1439
  privacy................................................................................................................ 1440

CSCF Enforce Codec Policy Configuration Mode Commands .......... 1441
  dynamic-codec..................................................................................................... 1443
end ....................................................................................................................... 1445
exit ......................................................................................................................... 1446
static-codec ........................................................................................................... 1447

CSCF IFC SPT Group Mode Commands ......................................................... 1449
end ....................................................................................................................... 1450
exit ......................................................................................................................... 1451
spt-condition ........................................................................................................ 1452

CSCF IFC Trigger Point Mode Commands ................................................ 1453
end ....................................................................................................................... 1454
exit ......................................................................................................................... 1455
spt-group ................................................................................................................ 1456

CSCF ISC Template Configuration Mode Commands .................................. 1457
cnsa ....................................................................................................................... 1458
end ....................................................................................................................... 1460
exit ......................................................................................................................... 1461
filter-criteria ......................................................................................................... 1462

CSCF Last Route Profile Criteria Configuration Mode Commands .......... 1463
county-name .......................................................................................................... 1464
end ....................................................................................................................... 1465
exit ......................................................................................................................... 1466
lro-number ............................................................................................................ 1467

CSCF Peer Servers Configuration Mode Commands .............................. 1469
end ....................................................................................................................... 1470
exit ......................................................................................................................... 1471
hunting-method ..................................................................................................... 1472
server ..................................................................................................................... 1473

CSCF Peer Server Monitoring Configuration Mode Commands .......... 1475
end ....................................................................................................................... 1477
exit ......................................................................................................................... 1478
ims-capable ........................................................................................................... 1479
lro-selection-profile ........................................................................................... 1480
mode .................................................................................................................... 1481
monitor-status ...................................................................................................... 1482
nw-session-template ............................................................................................ 1483

CSCF Policy Configuration Mode Commands ............................................ 1485
aor-policy-rules ..................................................................................................... 1486
end ....................................................................................................................... 1487
exit ......................................................................................................................... 1488
service-policy-rules .............................................................................................. 1489

CSCF Policy Rules Configuration Mode Commands .................................... 1491
allow-noauth ......................................................................................................... 1492
allow-unsecure ..................................................................................................... 1493
authorization .......................................................................................................... 1494
end ....................................................................................................................... 1495
enforce-codec-policy ........................................................................................... 1496
exit ......................................................................................................................... 1497
max-cscf-concurrent-sessions ........................................................................... 1498
policy ................................................................................................................... 1499
qos ......................................................................................................................... 1501
video-sessions ...................................................................................................... 1502
CSCF Proxy-CSCF Configuration Mode Commands ......................... 1503
allow .................................................................................. 1504
diameter .............................................................................. 1505
emergency-sessions ............................................................. 1508
end ...................................................................................... 1509
exit ...................................................................................... 1510
interrogating-cscf-role ......................................................... 1511
message-max-size ................................................................. 1511
network-id .......................................................................... 1513
peer-sbc .............................................................................. 1514
plmn-id ............................................................................... 1515
reg-service-route ................................................................. 1516
reliable-prov-resp ............................................................... 1517
restoration-procedure ......................................................... 1518
security-parameters ............................................................ 1519
sigcomp .............................................................................. 1520
sip-header ............................................................................ 1521
sip-param ............................................................................. 1522
store-session-path ............................................................... 1523
CSCF Routes Configuration Mode Commands ......................... 1525
after ..................................................................................... 1526
before ................................................................................... 1527
end ...................................................................................... 1528
exit ...................................................................................... 1529
route ................................................................................... 1530
CSCF Service Configuration Mode Commands ........................... 1537
access-service ................................................................. 1538
access-type ........................................................................ 1539
allow-dereg ......................................................................... 1541
bind .................................................................................... 1542
charging ............................................................................ 1544
cnsa-media-profile .............................................................. 1545
core-service ........................................................................ 1546
default-aor-domain ............................................................ 1548
direct-call-on-media-loss ..................................................... 1549
emergency-cscf ................................................................. 1550
end ...................................................................................... 1551
exit ...................................................................................... 1551
history-info ........................................................................ 1552
interface ............................................................................ 1553
ipv4-ipv6-interworking ...................................................... 1554
keepalive ............................................................................ 1555
li-packet-cable ................................................................... 1557
max-sipmsg-size ................................................................. 1559
media-bridging ................................................................... 1560
nat-policy ............................................................................ 1561
nat-pool ............................................................................. 1562
policy ............................................................................... 1563
policy-name ....................................................................... 1564
proxy-cscf ........................................................................ 1566
route ............................................................................... 1567
recursive-redirect-resp ....................................................... 1568
reject-on-cnsa-failure ....................................................... 1569
release-call-on-media-loss .................................................. 1570
rfc3261-proxy .................................................................. 1571
serving-cscf .................................................................... 1572
serving-cscf-list ................................................................. 1573
session-timer ................................................................. 1574
strict-outbound ............................................................. 1576
subscriber-policy-override ............................................. 1577
subscription ................................................................. 1578
tcp-proxy ........................................................................ 1580
threshold ......................................................................... 1581
timeout ............................................................................ 1582
transport-switching .......................................................... 1584
trusted-domain-entity ..................................................... 1585

CSCF Security Configuration Mode Commands ................. 1587
  auth-failure-weight ....................................................... 1588
  bad-request-weight ..................................................... 1589
  dos-prevention .......................................................... 1590
  end ............................................................................ 1591
  exit ............................................................................ 1592
  forking-contact-limit .................................................... 1593
  greylist-duration ........................................................ 1594
  per-aor-failure-limit ..................................................... 1595
  per-ip-failure-limit ......................................................... 1596
  threshold-rate ........................................................... 1597

CSCF Serving-CSCF Configuration Mode Commands .......... 1599
  3gpp ........................................................................... 1600
  alias-indication .......................................................... 1601
  allow ......................................................................... 1602
  authentication ............................................................ 1603
  diversion-info ............................................................. 1605
  end ............................................................................ 1606
  exit ............................................................................ 1607
  ims-restoration ........................................................... 1608
  interrogating-cscf-role ............................................... 1609
  local-call-features ....................................................... 1610
  network-id ................................................................. 1611
  policy ......................................................................... 1612
  registration ................................................................. 1613
  reliable-prov-resp ....................................................... 1614
  sifc ........................................................................... 1615
  sip-header ................................................................. 1616
  sip-request ................................................................. 1617
  tas ............................................................................. 1619
  tas-service ................................................................. 1620

CSCF Session Template Configuration Mode Commands ....... 1621
  end ............................................................................ 1622
  exit ............................................................................ 1623
  inbound-cscf-acl .......................................................... 1624
  outbound-cscf-acl ........................................................ 1625
  policy-profile ............................................................. 1626
  route-list ................................................................. 1627
  translation-list ............................................................ 1628
  urn-service-list .......................................................... 1629

CSCF Signalling Compression Configuration Mode Commands .... 1631
  compression-mode ......................................................... 1633
  decompression-memory-size ........................................ 1634
CSCF URI Readdress Configuration Mode Commands ............................................ 1639
alias-indication .................................................................................. 1640
as-call .............................................................................................. 1641
authentication .................................................................................. 1642
diversion-info .................................................................................. 1644
emergency-sessions ......................................................................... 1645
end ...................................................................................................... 1646
exit ...................................................................................................... 1647
ims-restoration .................................................................................. 1648
registration ...................................................................................... 1649
reliable-prov-resp ........................................................................... 1650
sifc ...................................................................................................... 1651
sigcomp ............................................................................................. 1652
tas ....................................................................................................... 1653
tas-service ........................................................................................ 1654
CSCF Translation Configuration Mode Commands ........................................ 1655
after .................................................................................................... 1656
before .................................................................................................. 1657
end ...................................................................................................... 1658
exit ...................................................................................................... 1659
uri-readdress ..................................................................................... 1660
CSCF URI Readdress Configuration Mode Commands ........................................ 1663
action .................................................................................................. 1664
end ...................................................................................................... 1666
exit ...................................................................................................... 1667
CSCF URN List Configuration Mode Commands ........................................... 1669
cscf-urn-service-mapping .................................................................. 1670
end ...................................................................................................... 1671
exit ...................................................................................................... 1672
CSS Delivery Sequence Configuration Mode Commands .................................. 1673
end ...................................................................................................... 1674
exit ...................................................................................................... 1675
redirect service (any) ........................................................................ 1676
CSS Service Configuration Mode Commands ............................................. 1677
end ...................................................................................................... 1678
exit ...................................................................................................... 1679
recovery .............................................................................................. 1680
server-interface .................................................................................. 1681
DHCP Service Configuration Mode Commands ........................................... 1683
bind ...................................................................................................... 1684
default ................................................................................................. 1686
dhep client-identifier ........................................................................ 1688
dhep deadtime .................................................................................. 1689
dhep detect-dead-server .................................................................. 1690
dhep ip vrf ......................................................................................... 1691
dhep server ........................................................................................ 1692
dhep server selection-algorithm ............................................................. 1693
end ...................................................................................................... 1694
exit................................................................. 1695
lease-duration................................................. 1696
max-retransmissions........................................ 1697
retransmission-timeout................................. 1698
T1-threshold.................................................. 1699
T2-threshold.................................................. 1700

Diameter Endpoint Configuration Mode Commands................. 1701
cea-timeout.................................................... 1702
connection retry-timeout................................. 1703
connection timeout........................................ 1704
device-watchdog-request................................. 1705
dpa-timeout.................................................... 1706
end............................................................... 1707
exit.............................................................. 1708
max-outstanding............................................. 1709
origin address............................................... 1710
origin host.................................................... 1711
origin realm................................................... 1712
peer.............................................................. 1713
response-timeout.......................................... 1714
route-entry.................................................... 1715
route-failure................................................ 1716
tls............................................................... 1717
use-proxy....................................................... 1718
watchdog-timeout.......................................... 1719

DLCI Configuration Mode Commands........................................... 1725
bind link......................................................... 1726
end.............................................................. 1727
exit.............................................................. 1728
shaping........................................................ 1729
shutdown....................................................... 1730

DNS Client Configuration Mode Commands............................... 1731
bind address................................................... 1732
cache algorithm............................................. 1733
cache size...................................................... 1734
cache ttl....................................................... 1735
end.............................................................. 1736
exit.............................................................. 1737
resolver....................................................... 1738
round-robin answer....................................... 1739

EAP Authentication Configuration Mode Commands....................... 1741
eap-aka........................................................ 1742
eap-gtc.......................................................... 1743
eap-md5.......................................................... 1744
end.............................................................. 1745
exit.............................................................. 1746

EAP Configuration Mode Commands........................................... 1747
end.............................................................. 1748
exit.............................................................. 1749
max-retry....................................................... 1750
mode............................................................ 1751
EAP Mode Configuration Mode Commands............................... 1753
EDR Format Configuration Mode Commands ........................................ 1757
attribute ................................................................. 1758
end................................................................. 1759
event-label .......................................................... 1765
exit................................................................. 1766
rule-variable ...................................................... 1768
EDR Module Configuration Mode Commands ............................. 1777
cdr ................................................................. 1778
end................................................................. 1781
exit................................................................. 1782
file ................................................................. 1783
eGTP Service Configuration Mode Commands .......................... 1789
associate ............................................................ 1790
end................................................................. 1791
exit................................................................. 1792
gtpc ........................................................-------- 1793
interface-type ..................................................... 1795
validation-mode .................................................. 1796
Ethernet Interface Configuration Mode Commands .................. 1797
crypto-map ........................................................ 1798
description ........................................................ 1799
end................................................................. 1800
exit................................................................. 1801
ip .......................................................... 1802
ip mtu .............................................................. 1804
ip ospf authentication-key ....................................... 1805
ip ospf authentication-type ...................................... 1806
ip ospf cost ....................................................... 1807
ip ospf intervals .................................................. 1808
ip ospf message-digest-key ...................................... 1810
ip ospf network ................................................... 1811
ip ospf priority ................................................... 1812
ipv6 access-group ............................................... 1813
ipv6 address ...................................................... 1815
ipv6 router advertisement ........................................ 1816
policy-forward .................................................. 1817
pool-share-protocol ............................................. 1818
port-switch-on-L3-fail ........................................... 1820
vlan-map .......................................................... 1822
Ethernet Port Configuration Mode Commands ....................... 1823
bind interface ...................................................... 1824
default ............................................................. 1825
description ........................................................ 1826
end................................................................. 1827
exit................................................................. 1828
flow-control ......................................................... 1829
ingress-mode ...................................................... 1830
link aggregation ................................................... 1831
media .......................................................... 1833
medium .......................................................... 1834
preferred slot
shutdown
snmp trap link-status
srp virtual-mac-address
threshold high-activity
threshold monitoring
threshold rx-utilization
threshold tx-utilization
vlan

Exec Mode Commands (A-C) ................................................................. 1849

aaa test ................................................................. 1850
active-charging service .................................................. 1852
alarm ................................................................. 1853
autoconfirm ........................................................... 1854
bulkstats force ......................................................... 1855
card halt ............................................................. 1856
card lc switch ......................................................... 1857
card lc upgrade ....................................................... 1858
card psc .............................................................. 1859
card psc upgrade ..................................................... 1861
card reboot .......................................................... 1862
card restart .......................................................... 1864
card smc .............................................................. 1866
card smc upgrade ..................................................... 1868
card spio .............................................................. 1869
cdr-push .............................................................. 1870
clear ................................................................. 1871
clear aaa .............................................................. 1872
clear active-charging analyzer statistics ..................... 1873
clear active-charging charging-action statistics .......... 1877
clear active-charging content-filtering category statistics 1878
clear active-charging credit-control statistics .............. 1879
clear active-charging edir-format statistics ................. 1880
clear active-charging edir-udr-file statistics ............... 1881
clear active-charging firewall statistics ..................... 1882
clear active-charging firewall track-list ..................... 1884
clear active-charging fw-and-nat policy statistics ......... 1885
clear active-charging group-of-ruledefs statistics .......... 1886
clear active-charging nat statistics ......................... 1887
clear active-charging rulebase statistics .................... 1888
clear active-charging ruledef statistics ..................... 1889
clear active-charging subsystem ............................... 1890
clear active-charging url-blacklisting statistics .......... 1891
clear administrator ................................................. 1892
clear alarm .......................................................... 1893
clear asngw-service ............................................... 1894
clear asnp-service ................................................. 1895
clear apn statistics ............................................... 1896
clear bcmcs statistics ............................................. 1897
clear blacklisted-gtpu-bind-address ......................... 1898
clear bssap+ statistics ............................................ 1899
clear bulkstats ...................................................... 1900
clear config ........................................................ 1901
clear congestion-control statistics ......................... 1902
clear content-filtering category statistics ................. 1904
clear crash .......................................................... 1905
clear credit-control statistics .................................. 1906
clear crypto ....................................................... 1907
clear csf service .................................................. 1909
clear csf sessions ................................................. 1911
clear csf sip ....................................................... 1912
clear csf subscription ............................................ 1913
clear diameter aaa-statistics .................................. 1914
clear diameter statistics ........................................ 1915
clear dhcpr statistics ............................................ 1916
clear dns-client ................................................... 1917
clear egtpc ......................................................... 1918
clear firewall flows .............................................. 1920
clear firewall ruledef ............................................ 1921
clear firewall statistics ......................................... 1922
clear gmm-sm statistics ......................................... 1923
clear gtpr statistics .............................................. 1925
clear gtpp statistics .............................................. 1927
clear gtpp storage-server local file statistics .............. 1928
clear gtpp storage-server statistics .......................... 1929
clear gtpr statistics .............................................. 1930
clear hd-storage-policy ......................................... 1931
clear hsgw-service .............................................. 1932
clear ims-authorization ........................................ 1933
clear ip access-group statistics ............................... 1934
clear ip arp ........................................................ 1935
clear ip bgp peer .................................................. 1936
clear ip localhosts ................................................. 1937
clear ip ospf process .............................................. 1938
clear ipv6 neighbors .............................................. 1939
clear l2tp .......................................................... 1940
clear lawful-intercept ............................................ 1942
clear lma-service statistics ..................................... 1943
clear local-user .................................................... 1944
clear mag-service statistics .................................... 1945
clear maximum-temperatures ................................. 1946
clear mipfa statistics ............................................. 1947
clear mipha statistics ............................................. 1948
clear mme-service db statistics ............................... 1949
clear mme-service db record .................................... 1950
clear mme-service statistics .................................... 1951
clear mme-service statistics .................................... 1953
clear multicast-sessions ........................................ 1955
clear orbem statistics ........................................... 1957
clear pdg-service statistics ..................................... 1958
clear pgw-service ................................................ 1959
clear port .......................................................... 1960
clear ppp statistics ................................................. 1962
clear prepaid 3gpp2 statistics .................................. 1963
clear prepaid wimax .............................................. 1964
clear qos npu stats ................................................. 1965
clear radius accounting archive ............................... 1966
clear radius counters ............................................ 1967
clear rohc statistics ............................................. 1968
clear rp service-option ......................................... 1969
clear rp statistics ................................................ 1970
Exec Modes Commands (D-S) .................................................. 2001

clear session disconnect-reasons ............................................. 1971
clear session setuptime .......................................................... 1972
clear session subsystem ......................................................... 1973
clear sgtpu statistics .............................................................. 1974
clear sgw-service statistics ..................................................... 1975
clear snmp trap ................................................................. 1976
clear srp checkpoint statistics ................................................ 1977
clear srp statistics ............................................................... 1978
clear subscribers .................................................................... 1979
clear super-charger ............................................................... 1989
cli ....................................................................................... 1990
clock set .............................................................................. 1991
configure ............................................................................. 1992
context ................................................................................ 1994
copy ................................................................................... 1995

crash copy ........................................................................... 1997
crypto-group ....................................................................... 1999
delasit .................................................................................. 2001
debug ................................................................................... 2002
debug ip ............................................................................... 2003
debug ip bgp ......................................................................... 2004
debug ip ospf all ................................................................... 2006
debug ip ospf event ................................................................ 2007
debug ip ospf ism .................................................................. 2009
debug ip ospf lsa ................................................................... 2010
debug ip ospf nsm .................................................................. 2012
debug ip ospf packet ............................................................... 2013
debug ip ospf route ................................................................ 2015
debug ip ospf router .............................................................. 2016
default terminal ..................................................................... 2017
delete .................................................................................... 2018
dhcp force ............................................................................. 2019
dhcp test ............................................................................... 2020
diameter disable endpoint ....................................................... 2021
diameter enable endpoint ....................................................... 2022
diameter reset connection ..................................................... 2023
diameter reset route failure .................................................. 2024
directory ............................................................................... 2026
disable ............................................................................... 2028
dns-client ............................................................................. 2029
enable .................................................................................. 2031
exit ...................................................................................... 2032
filesystem format ................................................................. 2033
filesystem repair ................................................................. 2034
gtpc test echo ....................................................................... 2035
gtp interim now ................................................................. 2037
gtp interin now active-charging egcdr ................................. 2040
gtp storage-server commit .................................................... 2042
gtp test ............................................................................... 2043
gtpu test echo ..................................................................... 2045
gtpv0 test echo .................................................................... 2047
hd raid .................................................................................. 2049
host .................................................................................... 2051
interface sent gratuitous-arp ............................................... 2052
lawful-intercept ................................................................. 2053

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01
lawful-intercept packet-cable .............................. 2057
lawful-intercept ssdf ......................................... 2059
logging active ................................................. 2061
logging filter .................................................. 2063
logging trace .................................................. 2068
logs checkpoint ............................................... 2070
mkdir .......................................................... 2071
monitor protocol .............................................. 2072
monitor subscriber ........................................... 2076
newcall policy ................................................. 2080
password change .............................................. 2084
ping .............................................................. 2087
ping6 ............................................................ 2089
ppp echo-test ................................................. 2090
radius interim .................................................. 2092
radius test ...................................................... 2093
reload ............................................................ 2095
rename ........................................................... 2096
reveal disabled commands .................................... 2098
rlogin ............................................................ 2099
rmmdir .......................................................... 2100
rotate-hd-file ................................................. 2104
save configuration .......................................... 2102
save logs ....................................................... 2104
session trace subscriber ..................................... 2110
setup ............................................................ 2113
sgsn imsimgr .................................................... 2114
sgsn offload .................................................... 2115
shutdown ....................................................... 2117
sleep .............................................................. 2118
srp initiate-switchover ..................................... 2119
srp reset-auth-probe-fail ................................... 2120
srp terminate-post-process .................................. 2121
srp validate-configuration .................................... 2122
ssh .............................................................. 2123
start crypto security-association .............................. 2124

**Exec Mode (T-Z)** ........................................ 2125
telnet .......................................................... 2126
terminal ......................................................... 2127
test alarm ....................................................... 2128
timestamps ...................................................... 2129
traceroute ....................................................... 2130
update active-charging ...................................... 2133
update cscf ..................................................... 2135
update firewall policy ....................................... 2136
update ip ......................................................... 2137
update qos policy map ....................................... 2138
update qos tft .................................................. 2140
upgrade ......................................................... 2141
upgrade content-filtering .................................... 2143
upgrade url-blacklisting database .......................... 2144

**Exec Mode Show Commands (A-C)** .......................... 2145
show ............................................................ 2146
show aaa ........................................................ 2147
show active-charging analyzer statistics ................................................................. 2148
show active-charging bandwidth-policy ................................................................. 2150
show active-charging charging-action ................................................................. 2151
show active-charging content-filtering category policy-id .................................. 2153
show active-charging content-filtering category statistics .................................. 2154
show active-charging content-filtering server-group .......................................... 2156
show active-charging credit-control ................................................................. 2158
show active-charging edr-format .................................................................. 2160
show active-charging edr-udr-file .................................................................. 2161
show active-charging file-space-usage ................................................................. 2162
show active-charging firewall statistics .............................................................. 2163
show active-charging firewall track-list .............................................................. 2165
show active-charging flows ............................................................................. 2166
show active-charging fw-and-nat policy ............................................................ 2172
show active-charging group-of-prefixed-urls .................................................... 2174
show active-charging group-of-rulesdefs ........................................................... 2175
show active-charging nat statistics ................................................................. 2177
show active-charging p2p-dynamic-rules ........................................................... 2179
show active-charging packet-filter .................................................................. 2180
show active-charging rulebase ....................................................................... 2181
show active-charging ruledef ........................................................................... 2183
show active-charging service .......................................................................... 2185
show active-charging sessions ........................................................................ 2186
show active-charging subsystem ..................................................................... 2191
show active-charging timedef .......................................................................... 2192
show active-charging udr-format ..................................................................... 2194
show active-charging url-blacklisting statistics .............................................. 2195
show active-charging xheader-format .............................................................. 2196
show administrators ...................................................................................... 2197
show alarm ....................................................................................................... 2198
show apn .......................................................................................................... 2200
show apn counter ip-allocation ....................................................................... 2201
show apn statistics ......................................................................................... 2202
show asngw-service ...................................................................................... 2203
show asngw-service session ......................................................................... 2205
show asngw-service session counters ............................................................... 2207
show asngw-service statistics ........................................................................ 2209
show asnpc-service ......................................................................................... 2211
show asnpc-service session .......................................................................... 2213
show asnpc-service session counters ............................................................... 2215
show asnpc-service session counters verbose ............................................... 2217
show asnpc-service statistics ....................................................................... 2219
show asnpc-service statistics verbose ............................................................. 2220
show banner ..................................................................................................... 2222
show bcmcs counters ...................................................................................... 2223
show bcmcs statistics ..................................................................................... 2224
show boot ......................................................................................................... 2225
show bssap+ statistics ..................................................................................... 2226
show bulkstats ................................................................................................ 2228
show card .......................................................................................................... 2230
show cli ........................................................................................................... 2232
show clock ....................................................................................................... 2233
show configuration ......................................................................................... 2234
show configuration errors ............................................................................... 2236
show congestion-control ............................................................................... 2239
show content-filtering category database ....................................................... 2241
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show content-filtering category policy-id</td>
<td>2243</td>
</tr>
<tr>
<td>show content-filtering category statistics</td>
<td>2244</td>
</tr>
<tr>
<td>show content-filtering category url</td>
<td>2246</td>
</tr>
<tr>
<td>show content-filtering server-group</td>
<td>2248</td>
</tr>
<tr>
<td>show context</td>
<td>2249</td>
</tr>
<tr>
<td>show cpu</td>
<td>2250</td>
</tr>
<tr>
<td>show crash</td>
<td>2252</td>
</tr>
<tr>
<td>show credit-control sessions</td>
<td>2253</td>
</tr>
<tr>
<td>show credit-control statistics</td>
<td>2254</td>
</tr>
<tr>
<td>show crypto group</td>
<td>2255</td>
</tr>
<tr>
<td>show crypto ikev1</td>
<td>2256</td>
</tr>
<tr>
<td>show crypto ikev2-ikesa security-associations summary</td>
<td>2257</td>
</tr>
<tr>
<td>show crypto ipsec</td>
<td>2258</td>
</tr>
<tr>
<td>show crypto ipsec transform-set</td>
<td>2260</td>
</tr>
<tr>
<td>show crypto isakmp keys</td>
<td>2261</td>
</tr>
<tr>
<td>show crypto isakmp policy</td>
<td>2262</td>
</tr>
<tr>
<td>show crypto isakmp security-associations</td>
<td>2263</td>
</tr>
<tr>
<td>show crypto managers</td>
<td>2264</td>
</tr>
<tr>
<td>show crypto map</td>
<td>2266</td>
</tr>
<tr>
<td>show crypto statistics</td>
<td>2268</td>
</tr>
<tr>
<td>show crypto transform-set</td>
<td>2269</td>
</tr>
<tr>
<td>show cscf nat</td>
<td>2270</td>
</tr>
<tr>
<td>show cscf peer-servers</td>
<td>2271</td>
</tr>
<tr>
<td>show cscf service</td>
<td>2272</td>
</tr>
<tr>
<td>show cscf sessions</td>
<td>2275</td>
</tr>
<tr>
<td>show cscf sip</td>
<td>2278</td>
</tr>
<tr>
<td>show cscf tcp</td>
<td>2280</td>
</tr>
<tr>
<td>show css delivery-sequence</td>
<td>2282</td>
</tr>
<tr>
<td>show css server</td>
<td>2283</td>
</tr>
<tr>
<td>show css service</td>
<td>2284</td>
</tr>
</tbody>
</table>

**Exec Mode Show Commands (D-G)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dhcp</td>
<td>2286</td>
</tr>
<tr>
<td>show dhcp statistics</td>
<td>2288</td>
</tr>
<tr>
<td>show dhcp-service</td>
<td>2289</td>
</tr>
<tr>
<td>show dhcp status</td>
<td>2290</td>
</tr>
<tr>
<td>show diameter aaa-statistics</td>
<td>2291</td>
</tr>
<tr>
<td>show diameter accounting servers aaa-group</td>
<td>2292</td>
</tr>
<tr>
<td>show diameter authentication servers aaa-group</td>
<td>2293</td>
</tr>
<tr>
<td>show diameter endpoint</td>
<td>2294</td>
</tr>
<tr>
<td>show diameter endpoints</td>
<td>2295</td>
</tr>
<tr>
<td>show diameter message-queue</td>
<td>2296</td>
</tr>
<tr>
<td>show diameter peers</td>
<td>2298</td>
</tr>
<tr>
<td>show diameter route status</td>
<td>2300</td>
</tr>
<tr>
<td>show diameter route table</td>
<td>2302</td>
</tr>
<tr>
<td>show diameter statistics</td>
<td>2303</td>
</tr>
<tr>
<td>show dns-client</td>
<td>2304</td>
</tr>
<tr>
<td>show dynamic-policy statistics</td>
<td>2306</td>
</tr>
<tr>
<td>show egtpc peers</td>
<td>2307</td>
</tr>
<tr>
<td>show egtp-service</td>
<td>2309</td>
</tr>
<tr>
<td>show egtpc sessions</td>
<td>2310</td>
</tr>
<tr>
<td>show egtpc statistics</td>
<td>2312</td>
</tr>
<tr>
<td>show external-inline-servers</td>
<td>2314</td>
</tr>
<tr>
<td>show fa-service</td>
<td>2315</td>
</tr>
<tr>
<td>show fans</td>
<td>2316</td>
</tr>
<tr>
<td>show file</td>
<td>2317</td>
</tr>
</tbody>
</table>
show firewall flows ................................................................. 2319
show firewall ruledef .............................................................. 2320
show firewall statistics ........................................................... 2321
show freeze-pmsi imsi ............................................................. 2322
show ggsn-service ............................................................... 2323
show ggsn-service gsn-table .................................................... 2324
show global-title-translation ................................................... 2325
show gmm-sm statistics .......................................................... 2326
show gprs-service ............................................................... 2329
show gs-service ....................................................................... 2330
show gtpc .................................................................................. 2331
show gtpc statistics ............................................................... 2333
show gtpp accounting ............................................................. 2335
show gtpp counters ............................................................... 2336
show gtpp group ....................................................................... 2337
show gtpp statistics ............................................................... 2338
show gtpp storage-server ......................................................... 2339
show gtpp storage-server ......................................................... 2341
show gtpu-service ................................................................. 2342

Exec Modes Show Commands (H-L) ........................................ 2343
show ha-service ....................................................................... 2344
show hardware ......................................................................... 2345
show hd raid ............................................................................. 2347
show hd-storage-policy ........................................................... 2348
show hnbgw counters ............................................................. 2349
show hnbgw statistics hnbgw-service ....................................... 2350
show hnbgw statistics hnbid ..................................................... 2352
show hnbgw-service .............................................................. 2354
show hsgw-service ............................................................... 2355
show ims-authorization policy-control .................................... 2356
show ims-authorization policy-gate .......................................... 2358
show ims-authorization servers .............................................. 2360
show ims-authorization service .............................................. 2361
show ims-authorization sessions .............................................. 2363
show ip ....................................................................................... 2365
show ip as-path-access-list .................................................... 2367
show ip bgp ............................................................................. 2368
show ip interface ..................................................................... 2368
show ip ospf ............................................................................. 2370
show ip policy-forward .......................................................... 2372
show ip pool ............................................................................. 2374
show ip ipsi .............................................................................. 2375
show ip ipsi ..... show ip ipms status ............................................ 2378
show ipms status ................................................................. 2379
show ips ................................................................................... 2380
show ipv6 .................................................................................. 2382
show ipv6 pool ......................................................................... 2384
show iups-service ...................................................................... 2385
show 12tp sessions ............................................................... 2387
show 12tp statistics ............................................................... 2389
show 12tp tunnels ................................................................. 2390
show lawful-intercept ............................................................ 2392
show lac-service ................................................................. 2394
show leds .................................................................................. 2395
show license information ....................................................... 2396
show linecard information ...................................................... 2397
show lma-service
show lns-service
show local-user
show logging
show logs

Exec Mode Show Commands (M-P) .................................................. 2411

show mag-service
show map-service
show map statistics
show maximum-temperatures
show mbms bearer-service
show mipfa
show mipha
show mipv6ha
show mme-hss service
show mme-hss session
show mme-service
show mme-service db statistics
show mme-service db record
show mme-service enodeb-association
show mme-service session
show mme-service statistics
show multicast-sessions
show network-requested-pdp-context
show network-service-entity
show nw-reachability server
show ntp
show orbem
show patch-progress
show pdg-service
show pdg-service statistics
show pdif-service
show pdsm-service
show pgw-service
show port
show power
show ppp
show prepaid 3gpp2
show prepaid wimax
show profile-id-qci-mapping

Exec Mode Show Commands (Q-S) ............................................... 2467

show qci-qos-mapping
show qos npu inter-subscriber traffic
show qos npu stats
show radius
show radius charging servers
show radius client
show radius counters
show resources
show rohc counters
show rohc statistics
show route-map
show rp
show rp service-option
show rp statistics
show rsvp counters ................................................................. 2487
show rsvp statistics ............................................................. 2488
show sccp-network ............................................................... 2489
show sccp statistics .............................................................. 2490
show session counters historical ........................................... 2491
show session counters pcf-summary ....................................... 2494
show session disconnect-reasons .......................................... 2495
show session duration .......................................................... 2497
show session progress .......................................................... 2500
show session recovery status ............................................... 2503
show session setup-time ....................................................... 2504
show session subsystem ....................................................... 2505
show session trace .............................................................. 2508
show sgsn-operator-policy .................................................... 2510
show sgsn-service ............................................................... 2511
show sgsn-sessmgr .............................................................. 2512
show sgtp-service ............................................................... 2513
show sgtpc statistics ............................................................. 2515
show sgtpu statistics ............................................................. 2516
show sgw-service ............................................................... 2518
show snmp ........................................................................ 2519
show srp ............................................................................ 2521
show srp monitor ................................................................. 2523
show ss7-routing-domain ...................................................... 2524
show ssh key .................................................................... 2527
show subscribers .................................................................. 2528
show super-charger .............................................................. 2546
show support details ............................................................. 2547
show system uptime .............................................................. 2551

**Exec Mode Show Commands (T-Z)** ..................................... 2553

show task ........................................................................... 2554
show temperature ............................................................... 2558
show terminal ..................................................................... 2559
show threshold .................................................................... 2560
show timing ........................................................................ 2561
show upgrade ...................................................................... 2562
show url-blacklisting database .............................................. 2563
show version ....................................................................... 2565

**FA Service Configuration Mode Commands** ........................... 2567

advertise ............................................................................. 2568
authentication aaa .............................................................. 2570
authentication mn-aaa .......................................................... 2571
authentication mn-ha ............................................................ 2573
bind ................................................................................. 2574
challenge-window .............................................................. 2576
default ............................................................................... 2577
default subscriber ............................................................... 2577
dynamic-ha-assignment ....................................................... 2580
dynamic-mip-key-update ...................................................... 2581
encapsulation allow gre ...................................................... 2582
end .................................................................................. 2583
exit .................................................................................. 2584
fa-ha-spi ........................................................................... 2585
gre .................................................................................... 2586
ha-monitor ......................................................................... 2589
idle-timeout-mode ................................................................. 2593
ignore-mip-key-data ................................................................. 2394
ignore-stale-challenge .............................................................. 2395
ip local-port ........................................................................... 2596
isakmp .................................................................................... 2597
limit-reg-lifetime ..................................................................... 2599
max-challenge-len .................................................................... 2600
mn-aaa-removal-indication ......................................................... 2601
multiple-reg ............................................................................ 2602
optimize tunnel-reassembly ......................................................... 2603
private-address allow-no-reverse-tunnel ....................................... 2604
proxy-mip .................................................................................. 2605
reg-timeout ............................................................................... 2607
reverse-tunnel ........................................................................... 2608
revocation ............................................................................... 2609
threshold reg-reply-error ............................................................. 2611

Firewall-and-NAT Policy Configuration Mode Commands .......... 2613
access-rule .............................................................................. 2614
end ......................................................................................... 2618
exit ......................................................................................... 2619
firewall dos-protection ............................................................... 2620
firewall flooding ....................................................................... 2622
firewall icmp-checksum-error ...................................................... 2624
firewall icmp-destination-unreachable-message-threshold ........ 2625
firewall icmp-fsm ..................................................................... 2627
firewall ip-reassembly-failure ..................................................... 2628
firewall malformed-packets ......................................................... 2629
firewall max-ip-packet-size ......................................................... 2630
firewall mime-flood .................................................................... 2631
firewall policy ........................................................................... 2632
firewall tcp-checksum-error ......................................................... 2634
firewall tcp-first-packet-non-syn .................................................. 2635
firewall tcp-fsm ....................................................................... 2636
firewall tcp-idle-timeout-action .................................................. 2637
firewall tcp-options-error .......................................................... 2638
firewall tcp-reset-message-threshold .......................................... 2639
firewall tcp-syn-flood-intercept .................................................. 2640
firewall tcp-syn-with-ecn-cwr ..................................................... 2642
firewall udp-checksum-error ....................................................... 2643
firewall validate-ip-options ......................................................... 2644
nat binding-record ................................................................... 2645
nat policy ................................................................................ 2646
nat private-ip-flow-timeout ......................................................... 2648
nat suppress-aaa-update ............................................................. 2649

Firewall Ruledef Configuration Mode Commands .................... 2651
bearer 3gpp apn ....................................................................... 2652
bearer 3gpp imsi ...................................................................... 2654
bearer username ....................................................................... 2655
create-log-record .................................................................... 2657
end ......................................................................................... 2658
exit ......................................................................................... 2659
icmp any-match ........................................................................ 2660
icmp code ................................................................................. 2661
icmp type .................................................................................. 2662
ip any-match ............................................................................. 2663

Cisco ASR 5000 Series Command Line Interface Reference
FTP Configuration Mode Commands ........................................... 2687
  end .......................................................... 2688
  exit ......................................................... 2689
  max servers ............................................ 2690
  timeout ................................................ 2691
GGSN Service Configuration Mode Commands ............................... 2693
  accounting ............................................. 2694
  authorize-with-hss .................................... 2695
  bind ....................................................... 2696
  cc behavior ............................................ 2698
  cc profile ............................................... 2699
  default .................................................. 2702
  dns-client .............................................. 2704
  echo-interval ......................................... 2705
  end ....................................................... 2707
  exit ..................................................... 2708
  fqdn ...................................................... 2709
  gtpc nsapi-in-create-pdp-response ..................... 2711
  gtpc private-extension ................................ 2712
  gtpc ran-procedure-ready-delay ...................... 2715
  gtpu echo-interval ................................... 2717
  gtpu reorder ........................................... 2718
  gtpu udp-checksum insert ................................ 2720
  guard-interval ........................................ 2721
  ip local-port ......................................... 2722
  ip qos-dscp ........................................... 2723
  max-retransmissions .................................. 2726
  mbms policy ............................................ 2727
  newcall ................................................. 2728
  path-failure .......................................... 2729
  plmn id .................................................. 2731
  plmn unlisted-sgsn .................................. 2732
  policy .................................................... 2734
  retransmission-timeout ................................ 2736
  setup-timeout ......................................... 2737
  sgsn address .......................................... 2738
  sgsn define-multiple-address-group .................. 2740
  sgsn multiple-address-group ......................... 2741
Global Configuration Mode Commands ...................................... 2743
  aaa accounting-overload-protection ................... 2744
  aaa default-domain ................................... 2745
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa domain-matching ignore-case</td>
<td>2746</td>
</tr>
<tr>
<td>aaa domain-matching imsi-prefix</td>
<td>2747</td>
</tr>
<tr>
<td>aaa large-configuration</td>
<td>2748</td>
</tr>
<tr>
<td>aaa last-resort</td>
<td>2749</td>
</tr>
<tr>
<td>aaa username-format</td>
<td>2750</td>
</tr>
<tr>
<td>active-charging service</td>
<td>2751</td>
</tr>
<tr>
<td>alarm</td>
<td>2753</td>
</tr>
<tr>
<td>arp</td>
<td>2754</td>
</tr>
<tr>
<td>autoconfirm</td>
<td>2755</td>
</tr>
<tr>
<td>autotless</td>
<td>2756</td>
</tr>
<tr>
<td>banner</td>
<td>2757</td>
</tr>
<tr>
<td>boot</td>
<td>2758</td>
</tr>
<tr>
<td>boot delay</td>
<td>2760</td>
</tr>
<tr>
<td>boot interface</td>
<td>2761</td>
</tr>
<tr>
<td>boot nameserver</td>
<td>2762</td>
</tr>
<tr>
<td>boot networkconfig</td>
<td>2764</td>
</tr>
<tr>
<td>boot system priority</td>
<td>2765</td>
</tr>
<tr>
<td>bulkstats</td>
<td>2767</td>
</tr>
<tr>
<td>ca-certificate</td>
<td>2770</td>
</tr>
<tr>
<td>card</td>
<td>2772</td>
</tr>
<tr>
<td>card-standby-priority</td>
<td>2773</td>
</tr>
<tr>
<td>cdr-multi-mode</td>
<td>2774</td>
</tr>
<tr>
<td>certificate</td>
<td>2775</td>
</tr>
<tr>
<td>cli</td>
<td>2776</td>
</tr>
<tr>
<td>clock</td>
<td>2777</td>
</tr>
<tr>
<td>congestion-control</td>
<td>2779</td>
</tr>
<tr>
<td>congestion-control overload-disconnect</td>
<td>2782</td>
</tr>
<tr>
<td>congestion-control policy</td>
<td>2784</td>
</tr>
<tr>
<td>congestion-control threshold</td>
<td>2786</td>
</tr>
<tr>
<td>content-filtering category database directory</td>
<td>2788</td>
</tr>
<tr>
<td>content-filtering category database max-versions</td>
<td>2792</td>
</tr>
<tr>
<td>content-filtering category database override</td>
<td>2793</td>
</tr>
<tr>
<td>context</td>
<td>2794</td>
</tr>
<tr>
<td>crash enable</td>
<td>2795</td>
</tr>
<tr>
<td>cs-network</td>
<td>2796</td>
</tr>
<tr>
<td>css acsmgr-selection-attempts</td>
<td>2798</td>
</tr>
<tr>
<td>css delivery-sequence</td>
<td>2800</td>
</tr>
<tr>
<td>css service</td>
<td>2801</td>
</tr>
<tr>
<td>default</td>
<td>2802</td>
</tr>
<tr>
<td>diameter-proxy ram-disk-limit</td>
<td>2803</td>
</tr>
<tr>
<td>end</td>
<td>2807</td>
</tr>
<tr>
<td>enforce imsi-min equivalence</td>
<td>2808</td>
</tr>
<tr>
<td>exit</td>
<td>2809</td>
</tr>
<tr>
<td>gtpp compression-process</td>
<td>2811</td>
</tr>
<tr>
<td>gtpp ram-disk-limit</td>
<td>2812</td>
</tr>
<tr>
<td>gtpp single-source</td>
<td>2813</td>
</tr>
<tr>
<td>global-title-translation address-map</td>
<td>2814</td>
</tr>
<tr>
<td>global-title-translation association</td>
<td>2816</td>
</tr>
<tr>
<td>hd raid</td>
<td>2817</td>
</tr>
<tr>
<td>hd storage-policy</td>
<td>2818</td>
</tr>
<tr>
<td>high-availability</td>
<td>2819</td>
</tr>
<tr>
<td>license</td>
<td>2820</td>
</tr>
<tr>
<td>line</td>
<td>2821</td>
</tr>
<tr>
<td>local-user allow-aaa-authentication</td>
<td>2823</td>
</tr>
<tr>
<td>local-user lockout-time</td>
<td>2824</td>
</tr>
<tr>
<td>local-user max-failed-logins</td>
<td>2825</td>
</tr>
<tr>
<td>local-user max-failed-logins</td>
<td>2826</td>
</tr>
</tbody>
</table>
task facility sessmgr .................................................................................................................. 2910
task facility acsmgr ................................................................................................................ 2912
terminal ................................................................................................................................... 2913
threshold .................................................................................................................................. 2915
threshold 10sec-cpu-utilization ............................................................................................. 2916
threshold aaa-acct-archive-size ............................................................................................. 2918
threshold aaa-acct-failure ....................................................................................................... 2920
threshold aaa-acct-failure-rate ............................................................................................... 2922
threshold aaa-auth-failure ....................................................................................................... 2924
threshold aaa-auth-failure-rate ............................................................................................... 2926
threshold aaa-retry-rate .......................................................................................................... 2928
threshold aaamgr-request-queue ............................................................................................ 2930
threshold asngw-auth-failure ................................................................................................... 2932
threshold asngw-handoff-denial ............................................................................................. 2934
threshold asngw-max-eap-retry .............................................................................................. 2936
threshold asngw-network-entry-denial .................................................................................... 2938
threshold asngw-r6-invalid-nai .............................................................................................. 2940
threshold asngw-session-setup-timeout .................................................................................. 2942
threshold asngw-session-timeout ............................................................................................ 2944
threshold call-reject-no-resource ......................................................................................... 2946
threshold call-setup ................................................................................................................ 2948
threshold call-setup-failure ..................................................................................................... 2950
threshold cpu-available-memory ............................................................................................ 2952
threshold cpu-load .................................................................................................................. 2954
threshold cpu-memory-usage .................................................................................................. 2956
threshold cpu-orbs-crit ........................................................................................................... 2958
threshold cpu-orbs-warn ......................................................................................................... 2960
threshold cpu-session-throughput .......................................................................................... 2962
threshold cdr-file-space .......................................................................................................... 2964
threshold contfilt-block ......................................................................................................... 2966
threshold contfilt-rating ........................................................................................................ 2967
threshold cpu-utilization ........................................................................................................ 2968
threshold dcca-bad-answer ..................................................................................................... 2970
threshold dcca-protocol-error ................................................................................................. 2972
threshold dcca-rating-failed .................................................................................................... 2974
threshold dcca-unknown-rating-group .................................................................................. 2976
threshold diameter diameter-retry-rate ................................................................................ 2978
threshold edr-file-space ......................................................................................................... 2980
threshold edr-udr-dropped flow control ................................................................................ 2982
threshold fw-deny-rule .......................................................................................................... 2984
threshold fw-dos-attack ......................................................................................................... 2985
threshold fw-drop-packet ....................................................................................................... 2986
threshold fw-no-rule ............................................................................................................... 2987
threshold license ................................................................................................................... 2988
threshold mgmt-cpu-memory-usage ....................................................................................... 2990
threshold mgmt-cpu-utilization .............................................................................................. 2992
threshold mme-attach-failure ................................................................................................. 2994
threshold mme-auth-failure .................................................................................................... 2996
threshold model .................................................................................................................... 2998
threshold monitoring ............................................................................................................. 3000
threshold nat-port-chunks-usage .......................................................................................... 3003
threshold packets-filtered-dropped ....................................................................................... 3006
threshold packets-forwarded-to-cpu ...................................................................................... 3008
threshold pdg-current-active-sessions ................................................................................... 3010
threshold pdg-current-sessions .............................................................................................. 3011
threshold pdif-current-sessions ............................................................................................. 3012
<table>
<thead>
<tr>
<th>Threshold</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold pdif-current-active-sessions</td>
<td>3013</td>
</tr>
<tr>
<td>threshold per-service-ggsn-sessions</td>
<td>3014</td>
</tr>
<tr>
<td>threshold per-service-gprs-pdp-sessions</td>
<td>3016</td>
</tr>
<tr>
<td>threshold per-service-gprs-sessions</td>
<td>3018</td>
</tr>
<tr>
<td>threshold per-service-ha-sessions</td>
<td>3020</td>
</tr>
<tr>
<td>threshold per-service-lns-sessions</td>
<td>3022</td>
</tr>
<tr>
<td>threshold per-service-pdsn-sessions</td>
<td>3024</td>
</tr>
<tr>
<td>threshold per-service-sgsn-pdp-sessions</td>
<td>3026</td>
</tr>
<tr>
<td>threshold per-service-sgsn-sessions</td>
<td>3028</td>
</tr>
<tr>
<td>threshold poll</td>
<td>3030</td>
</tr>
<tr>
<td>threshold poll asngw-auth-failure</td>
<td>3046</td>
</tr>
<tr>
<td>threshold poll asngw-handoff-denial</td>
<td>3047</td>
</tr>
<tr>
<td>threshold poll asngw-max-eap-retry</td>
<td>3048</td>
</tr>
<tr>
<td>threshold poll asngw-network-entry-denial</td>
<td>3049</td>
</tr>
<tr>
<td>threshold poll asngw-r6-invalid-nai</td>
<td>3050</td>
</tr>
<tr>
<td>threshold poll asngw-session-setup-timeout</td>
<td>3051</td>
</tr>
<tr>
<td>threshold poll asngw-session-timeout</td>
<td>3052</td>
</tr>
<tr>
<td>threshold poll cdr-file-space</td>
<td>3053</td>
</tr>
<tr>
<td>threshold poll contfilt-block</td>
<td>3054</td>
</tr>
<tr>
<td>threshold poll contfilt-rating</td>
<td>3055</td>
</tr>
<tr>
<td>threshold poll dcca-protocol-error</td>
<td>3056</td>
</tr>
<tr>
<td>threshold poll dcca-rating-failed</td>
<td>3057</td>
</tr>
<tr>
<td>threshold poll dcca-bad-answers</td>
<td>3058</td>
</tr>
<tr>
<td>threshold poll dcca-unknown-rating-group</td>
<td>3059</td>
</tr>
<tr>
<td>threshold poll diameter-retry-rate</td>
<td>3060</td>
</tr>
<tr>
<td>threshold poll edr-file-space</td>
<td>3061</td>
</tr>
<tr>
<td>threshold poll mme-attach-failure</td>
<td>3062</td>
</tr>
<tr>
<td>threshold poll mme-auth-failure</td>
<td>3063</td>
</tr>
<tr>
<td>threshold poll total-mme-sessions</td>
<td>3064</td>
</tr>
<tr>
<td>threshold poll port-rx-utilization</td>
<td>3065</td>
</tr>
<tr>
<td>threshold poll port-tx-utilization</td>
<td>3066</td>
</tr>
<tr>
<td>threshold poll port-high-activity</td>
<td>3067</td>
</tr>
<tr>
<td>threshold poll route-service</td>
<td>3068</td>
</tr>
<tr>
<td>threshold ppp-setup-fail-rate</td>
<td>3069</td>
</tr>
<tr>
<td>threshold route-service bgp-routes</td>
<td>3071</td>
</tr>
<tr>
<td>threshold rp-setup-fail-rate</td>
<td>3073</td>
</tr>
<tr>
<td>threshold spc-cpu-memory-usage</td>
<td>3075</td>
</tr>
<tr>
<td>threshold spc-cpu-utilization</td>
<td>3076</td>
</tr>
<tr>
<td>threshold storage-utilization</td>
<td>3077</td>
</tr>
<tr>
<td>threshold subscriber active</td>
<td>3079</td>
</tr>
<tr>
<td>threshold subscriber total</td>
<td>3081</td>
</tr>
<tr>
<td>threshold total-ggsn-sessions</td>
<td>3083</td>
</tr>
<tr>
<td>threshold total-gprs-sessions</td>
<td>3085</td>
</tr>
<tr>
<td>threshold total-gprs-pdp-sessions</td>
<td>3087</td>
</tr>
<tr>
<td>threshold total-ha-sessions</td>
<td>3089</td>
</tr>
<tr>
<td>threshold total-hsgw-sessions</td>
<td>3091</td>
</tr>
<tr>
<td>threshold total-lma-sessions</td>
<td>3093</td>
</tr>
<tr>
<td>threshold total-lns-sessions</td>
<td>3095</td>
</tr>
<tr>
<td>threshold total-mme-sessions</td>
<td>3097</td>
</tr>
<tr>
<td>threshold total-pdsn-sessions</td>
<td>3099</td>
</tr>
<tr>
<td>threshold total-pgw-sessions</td>
<td>3101</td>
</tr>
<tr>
<td>threshold total-sgw-sessions</td>
<td>3103</td>
</tr>
<tr>
<td>threshold total-sgsn-sessions</td>
<td>3105</td>
</tr>
<tr>
<td>threshold total-sgsn-pdp-sessions</td>
<td>3107</td>
</tr>
<tr>
<td>timestamps</td>
<td>3109</td>
</tr>
<tr>
<td>upgrade limit</td>
<td>3110</td>
</tr>
</tbody>
</table>
url-blacklisting database................................................................. 3112
Global Title Translation Address-Map Configuration Mode Commands 3115
associate ......................................................................................... 3116
description ....................................................................................... 3117
end ..................................................................................................... 3118
exit .................................................................................................... 3119
gt-address ......................................................................................... 3120
mode ................................................................................................. 3121
out-address ......................................................................................... 3122
Global Title Translation Association Configuration Mode Commands .. 3123
action ................................................................................................. 3124
description ......................................................................................... 3126
end ..................................................................................................... 3127
exit .................................................................................................... 3128
gt-format ........................................................................................... 3129
variant ............................................................................................... 3130
GPRS Service Configuration Mode Commands....................................... 3131
accounting ......................................................................................... 3132
associate-service ............................................................................... 3134
cc profile .......................................................................................... 3136
check-imei-timeout-action .................................................................. 3138
ciphering-algorithm ............................................................................ 3139
dns israu-mec-mnc-encoding ............................................................... 3141
end ..................................................................................................... 3142
exit .................................................................................................... 3143
gmm ................................................................................................. 3144
llc ....................................................................................................... 3147
nri ..................................................................................................... 3150
paging-policy ..................................................................................... 3152
peer-nsei ............................................................................................ 3154
plmn .................................................................................................. 3156
setup-timeout ..................................................................................... 3157
gsn-context-request ............................................................................ 3158
gsn-number ....................................................................................... 3159
sm ..................................................................................................... 3160
sdcep ................................................................................................. 3162
GRE Tunnel Interface Configuration Mode Commands ......................... 3163
destination ......................................................................................... 3164
end ..................................................................................................... 3165
exit .................................................................................................... 3166
keepalive ............................................................................................ 3167
source ............................................................................................... 3169
tos ..................................................................................................... 3170
ttl ...................................................................................................... 3172
Group of Ruledefs Configuration Mode Commands .............................. 3173
add-ruledef ....................................................................................... 3174
end ..................................................................................................... 3175
exit .................................................................................................... 3176
group-of-ruledefs-application .............................................................. 3177
Gs Service Configuration Mode Commands ........................................... 3179
associate-sccp-network ........................................................................ 3180
bssap+ ............................................................................................... 3181
## GT-Format1 Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>3193</td>
</tr>
<tr>
<td>exit</td>
<td>3194</td>
</tr>
<tr>
<td>max-retransmission</td>
<td>3195</td>
</tr>
<tr>
<td>non-pool-area</td>
<td>3196</td>
</tr>
<tr>
<td>pool-area</td>
<td>3197</td>
</tr>
<tr>
<td>sgn-number</td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td></td>
</tr>
<tr>
<td>vlr</td>
<td></td>
</tr>
</tbody>
</table>

## GT-Format2 Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>3199</td>
</tr>
<tr>
<td>exit</td>
<td>3200</td>
</tr>
<tr>
<td>translation-type</td>
<td>3201</td>
</tr>
</tbody>
</table>

## GT-Format3 Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>encoding-scheme</td>
<td>3203</td>
</tr>
<tr>
<td>end</td>
<td>3204</td>
</tr>
<tr>
<td>exit</td>
<td>3205</td>
</tr>
<tr>
<td>numbering-plan</td>
<td>3206</td>
</tr>
<tr>
<td>translation-type</td>
<td>3207</td>
</tr>
</tbody>
</table>

## GT-Format4 Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>encoding-scheme</td>
<td>3209</td>
</tr>
<tr>
<td>end</td>
<td>3210</td>
</tr>
<tr>
<td>exit</td>
<td>3211</td>
</tr>
<tr>
<td>nature-of-address</td>
<td>3212</td>
</tr>
<tr>
<td>numbering-plan</td>
<td>3213</td>
</tr>
<tr>
<td>translation-type</td>
<td>3214</td>
</tr>
</tbody>
</table>

## GTPP Server Group Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>gtp attribute</td>
<td>3217</td>
</tr>
<tr>
<td>gtp charging-agent</td>
<td>3218</td>
</tr>
<tr>
<td>gtp data-request sequence-numbers</td>
<td>3222</td>
</tr>
<tr>
<td>gtp deadtime</td>
<td>3224</td>
</tr>
<tr>
<td>gtp dead-server suppress-cdrs</td>
<td>3225</td>
</tr>
<tr>
<td>gtp detect-dead-server</td>
<td>3226</td>
</tr>
<tr>
<td>gtp dictionary</td>
<td>3227</td>
</tr>
<tr>
<td>gtp duplicate-hold-time</td>
<td>3228</td>
</tr>
<tr>
<td>gtp echo-interval</td>
<td>3229</td>
</tr>
<tr>
<td>gtp egcdr</td>
<td>3230</td>
</tr>
<tr>
<td>gtp error-response</td>
<td>3231</td>
</tr>
<tr>
<td>gtp max-cdrs</td>
<td>3232</td>
</tr>
<tr>
<td>gtp max-pdu-size</td>
<td>3233</td>
</tr>
<tr>
<td>gtp max-retries</td>
<td>3234</td>
</tr>
<tr>
<td>gtp mbms bucket</td>
<td>3235</td>
</tr>
<tr>
<td>gtp mbms interval</td>
<td>3236</td>
</tr>
<tr>
<td>gtp mbms tariff</td>
<td>3237</td>
</tr>
<tr>
<td>gtp mbms volume</td>
<td>3238</td>
</tr>
<tr>
<td>gtp redirection-allowed</td>
<td>3239</td>
</tr>
<tr>
<td>gtp redirection-disallowed</td>
<td>3240</td>
</tr>
<tr>
<td>gtp server</td>
<td>3241</td>
</tr>
<tr>
<td>gtp source-port-validation</td>
<td>3242</td>
</tr>
</tbody>
</table>

---

Contents
gtpp storage-server ......................................................... 3249
gtpp storage-server local file ........................................ 3250
gtpp storage-server max-retries .................................... 3252
gtpp storage-server mode ............................................. 3253
gtpp storage-server timeout .......................................... 3255
gtpp suppress-cdrs zero-volume-and-duration .................. 3256
gtpp timeout ............................................................ 3257
gtpp trigger .............................................................. 3258
gtpp transport-layer .................................................... 3261

GTP-U Service Configuration Mode Commands ................. 3263
bind ................................................................. 3264
echo-interval ......................................................... 3265
end ................................................................. 3266
exit ................................................................. 3267
extension-header ....................................................... 3268
max-retransmissions .................................................. 3269
path-failure detection-policy ....................................... 3270
retransmission-timeout .............................................. 3271

HA Proxy DNS Configuration Mode Commands .................. 3273
end ................................................................. 3274
exit ................................................................. 3275
pass-thru ............................................................. 3276
redirect ............................................................... 3277

HA Service Configuration Mode Commands ....................... 3279
aaa ................................................................. 3280
authentication ......................................................... 3281
bind ................................................................. 3283
binding-update ....................................................... 3285
default ............................................................. 3286
default subscriber ..................................................... 3288
encapsulation allow gre ............................................ 3289
deauth ............................................................. 3290
exit ................................................................. 3291
fa-ha-spi .......................................................... 3292
gre ................................................................. 3294
idle-timeout-mode ................................................... 3296
ip context-name ..................................................... 3297
ip local-port ......................................................... 3298
ip pool ............................................................. 3299
isakmp .............................................................. 3300
mn-ha-spi .......................................................... 3302
nat-traversal ........................................................ 3304
optimize tunnel-reassembly ....................................... 3305
policy bc-query-result ............................................ 3306
policy nw-reachability-fail ....................................... 3307
policy overload ....................................................... 3309
policy null-username .............................................. 3311
private-address allow-no-reverse-tunnel ......................... 3312
reg-lifetime ........................................................ 3313
reverse-tunnel ....................................................... 3314
revocation ........................................................... 3315
setup-timeout ......................................................... 3317
simul-bindings ....................................................... 3318
threshold init-rrq-rcvd-rate ....................................... 3319
HNB-RN PLMN Configuration Mode Commands............................. 3387
associate cs-network ............................................................... 3388
associate ps-network ............................................................... 3390
end .................................................................................. 3392
exit .................................................................................. 3393
rnc-id ............................................................................. 3394
HSGW Service Configuration Mode Commands .......................... 3397
associate ......................................................................... 3398
bind address ....................................................................... 3399
context-retention-timer ......................................................... 3401
data-available-indicator ......................................................... 3402
data-over-signaling .............................................................. 3403
dns-pgw ........................................................................... 3404
end .................................................................................. 3405
exit .................................................................................. 3406
fqdn ................................................................................ 3407
fragment .......................................................................... 3408
gre .................................................................................. 3412
ip ........................................................................................ 3415
max-retransmissions ............................................................. 3416
mobile-access-gateway ......................................................... 3417
plmn id ............................................................................ 3418
policy overload .................................................................. 3419
profile-id-qci-mapping ......................................................... 3421
registration-deny ................................................................. 3422
retransmission-timeout ........................................................ 3423
setup-timeout .................................................................... 3424
spi remote-address ............................................................... 3425
unauthorized-flows ............................................................... 3428
HSGW Service RoHC Configuration Mode Commands ............... 3429
cid-mode ........................................................................... 3430
end .................................................................................. 3431
exit .................................................................................. 3432
mrru ................................................................................ 3433
profile ............................................................................. 3434
IKEv2 Security Association Configuration Mode Commands ...... 3435
default .............................................................................. 3436
encryption ........................................................................ 3437
end .................................................................................. 3439
exit .................................................................................. 3440
group ............................................................................... 3441
hmac ............................................................................... 3442
lifetime ........................................................................... 3443
prf....................................................................................... 3444
IMS Authorization Service Configuration Mode Commands ........ 3445
end .................................................................................. 3446
exit .................................................................................. 3447
p-cscf discovery ................................................................. 3448
p-cscf table .......................................................................... 3450
policy-control .................................................................. 3452
qos-update-timeout ............................................................ 3453
reauth-trigger ................................................................. 3454
deny/permit (by IP packets) ................................................................. 3528
deny/permit (by TCP/UDP packets) .................................................... 3531
end ...................................................................................................... 3535
exit ...................................................................................................... 3536
readdress server ............................................................................... 3537
redirect context .............................................................................. 3540
redirect context (by IP address masking) .......................................... 3541
redirect context (any) .................................................................... 3543
redirect context (by host IP address) ............................................... 3545
redirect context (by source ICMP packets) ...................................... 3547
redirect context (by IP packets) ....................................................... 3550
redirect context (by TCP/UDP packets) .......................................... 3553
redirect css delivery-sequence ....................................................... 3557
redirect css service ........................................................................ 3558
redirect css service (any) ................................................................. 3559
redirect css service (by host IP address) ......................................... 3561
redirect css service (by ICMP packets) ........................................... 3563
redirect css service (by IP packets) ................................................ 3566
redirect css service (by source IP address masking) ..................... 3569
redirect css service (by TCP/UDP packets) .................................... 3571
redirect css service (for downlink, any) .......................................... 3575
redirect css service (for downlink, by host IP address) .................. 3577
redirect css service (for downlink, by ICMP packets) ..................... 3579
redirect css service (for downlink, by IP packets) .......................... 3582
redirect css service (for downlink, by source IP address masking) .. 3585
redirect css service (for uplink, any) .............................................. 3587
redirect css service (for uplink, by host IP address) ....................... 3592
redirect css service (for uplink, by ICMP packets) ......................... 3594
redirect css service (for uplink, by IP packets) ............................... 3596
redirect css service (for uplink, by source IP address masking) ....... 3599
redirect css service (for uplink, by TCP/UDP packets) ................. 3604
redirect nexthop ............................................................................. 3608
redirect nexthop (by IP address masking) ........................................ 3609
redirect nexthop (any) ................................................................... 3611
redirect nexthop (by host IP address) ............................................. 3613
redirect nexthop (by source ICMP packets) .................................... 3615
redirect nexthop (by IP packets) ..................................................... 3618
redirect nexthop (by TCP/UDP packets) ........................................ 3621
IPv6 to IPv4 Tunnel Interface Configuration Mode Commands .......... 3625
destination address ......................................................................... 3627
end ...................................................................................................... 3628
exit ...................................................................................................... 3629
mode .................................................................................................. 3630
source ............................................................................................... 3631
tos ....................................................................................................... 3632
ttl ......................................................................................................... 3633
ISAKMP Configuration Mode Commands ........................................ 3635
authentication .................................................................................. 3636
encryption ......................................................................................... 3637
end ...................................................................................................... 3638
exit ...................................................................................................... 3639
group ................................................................................................. 3640
hash .................................................................................................... 3641
lifetime ............................................................................................... 3642
IP VRF Context Configuration Mode Commands ........................................... 3643
end ................................................. 3644
exit .............................................. 3645
ip maximum-routes ............................................. 3646
mpls map-dscp-to-exp ...................................... 3647
mpls map-exp-to-dscp ...................................... 3649

IuPS Service Configuration Mode Commands ........................................... 3651
access-protocol ........................................... 3652
blacklist-timeout-gtpu-bind-addresses ........................................ 3653
end .............................................. 3654
exit .............................................. 3655
gtpu .............................................. 3656
iu-hold-connection ........................................ 3658
iu-recovery ......................................... 3659
iu-release-complete-timeout .................................. 3660
loss-of-radio-coverage ranap-cause ................................ 3661
plmn .............................................. 3662
rab-assignment-response-timeout ................................ 3664
radio-network-controller ..................................... 3665
relocation-complete-timeout .................................. 3666
reset .............................................. 3667
rnc .............................................. 3669
security-mode-complete-timeout ................................ 3670
srsn-context-response-timeout ................................ 3671
tigoc-timeout ......................................... 3672
tint-timeout ......................................... 3673

LAC Service Configuration Mode Commands ........................................... 3675
allow .............................................. 3676
bind .............................................. 3678
data sequence-number ...................................... 3679
default ........................................... 3680
hide-attributes ......................................... 3682
keepalive-interval ...................................... 3683
load-balancing ......................................... 3684
local-receive-window ...................................... 3685
max-retransmission ...................................... 3686
max-session-per-tunnel ..................................... 3687
max-tunnel-challenge-length .................................. 3688
max-tunnels .......................................... 3689
peer-Aws ........................................... 3690
proxy-lcp-authentication .................................... 3692
retransmission-timeout-first ................................ 3693
retransmission-timeout-max .................................. 3694
single-port-mode ........................................ 3695
snoop framed-ip-address .................................... 3696
trap .................................................. 3697
tunnel-authentication ........................................ 3698
tunnel selection-key .......................................... 3699

Line Configuration Mode Commands ...................................................... 3701
default ............................................. 3702
end .................................................. 3703
exit .................................................. 3704
length .............................................. 3705
Link Configuration Mode Commands

- arbitration
- end
- exit
- mtp2-issu-len
- lmp3-discard-priority
- mtp3-max-slt-try
- mtp3-msg-priority
- mtp3-msg-size
- mtp3-p1-qlen
- mtp3-p2-qlen
- mtp3-p3-qlen
- mtp3-test-pattern
- priority
- signaling-link-code
- sscf-nni-n1
- sscop-max-cc
- sscop-max-pd
- sscop-max-stat
- timeout

Linkset Configuration Mode Commands

- adjacent-point-code
- end
- exit
- link
- self-point-code

LMA Service Configuration Mode Commands

- aaa accounting
- bind address
- end
- exit
- refresh-advice-option
- refresh-interval-percent
- reg-lifetime
- revocation
- sequence-number-validate
- setup-timeout
- timestamp-replay-protection

LNS Service Configuration Mode Commands

- aaa accounting
- authentication
- avp map called-number apn
- bind
- data sequence-number
- default
- ip source-violation
- keepalive-interval
- local-receive-window
- max-retransmission
- max-session-per-tunnel
- max-tunnel-challenge-length
- max-tunnels
nai-construction domain ................................................. 3769
peer-lac ................................................................. 3770
proxy-lep-authentication ............................................ 3772
retransmission-timeout-first ......................................... 3773
retransmission-timeout-max .......................................... 3774
setup-timeout .......................................................... 3775
single-port-mode ...................................................... 3776
trap ........................................................................ 3777
tunnel-authentication .................................................. 3778
tunnel-switching ........................................................ 3779

Loopback Interface Configuration Mode Commands .............. 3781
description ..................................................................... 3782
end ............................................................................... 3783
exit .............................................................................. 3784
ip address ...................................................................... 3785
ip vrf ............................................................................ 3786
ipv6 address .................................................................. 3787

MAG Service Configuration Mode Commands ..................... 3789
bind address .................................................................... 3790
encapsulation .................................................................. 3792
end ............................................................................... 3793
exit .............................................................................. 3794
information-element-set ............................................... 3795
max-retransmissions ...................................................... 3796
reg-lifetime .................................................................. 3797
renew-percent-time ....................................................... 3798
retransmission-policy .................................................... 3799
retransmission-timeout ................................................ 3800

MAP Service Configuration Mode Commands .................... 3801
access-protocol ................................................................ 3802
application-context-name ............................................. 3803
auth-vectors .................................................................. 3805
end ............................................................................... 3806
equipment-identity-register ........................................... 3807
exit .............................................................................. 3809
hrl .............................................................................. 3810
policy ........................................................................... 3811
short-message-service .................................................. 3812

MIP HA Assignment Table Configuration Mode Commands ...... 3813
end ............................................................................... 3814
exit .............................................................................. 3815
hoa-range ..................................................................... 3816

MIPv6HA Service Configuration Mode Commands ............... 3817
aaa accounting ............................................................ 3818
bind .............................................................................. 3819
default .......................................................................... 3820
end ............................................................................... 3822
exit .............................................................................. 3823
refresh-advice-option ................................................... 3824
refresh-interval-percent ................................................. 3825
reg-lifetime .................................................................. 3826
sequence-number-validate ............................................. 3827
setup-timeout ............................................................... 3828
Network Service Entity - Peer NSEI Configuration Mode Commands .... 3885
bssgp-timer ........................................................................... 3886
end ......................................................................................... 3887
exit ......................................................................................... 3888
ns-vc .................................................................................... 3889

Network Service Entity- IP Local Configuration Mode Commands ....... 3891
all-nsvc-failure-action ............................................................. 3892
bssgp-timer ........................................................................... 3893
end ......................................................................................... 3894
exit ......................................................................................... 3895
max-ns-retransmissions .......................................................... 3896
ns-timer ................................................................................. 3897
nsvc-failure-action ................................................................. 3898
nsvl ....................................................................................... 3899
peer-network-service-entity .................................................... 3900
OSPF VRF Configuration Mode Commands ............................................. 3973

Out-Address Configuration Mode Commands ........................................... 3991

PDG Service Configuration Mode Commands ............................................ 4001

PDIF Service Configuration Mode Commands ............................................ 4019
PDSN Service Configuration Mode Commands.............................. 4039

aaa 3gpp2-service-option ................................................. 4040
access-flow traffic-validation .......................................... 4041
access-network ............................................................ 4042
airlink bad-sequence-number ........................................... 4043
allow alt-ppp .................................................................. 4044
always-on-indication ....................................................... 4045
authentication ............................................................... 4046
bind .............................................................................. 4048
bcmcs ............................................................................ 4050
data-available-indicator .................................................. 4052
data-over-signaling ........................................................ 4053
default ............................................................................ 4054
default subscriber ........................................................... 4058
dormant-transition ........................................................... 4059
end ................................................................................. 4060
exit ................................................................................. 4061
fragment .................................................................... 4062
gre ................................................................................... 4063
inter-pdsn-handoff mobility-event-indicator ....................... 4066
ip header-compression rohc ............................................... 4067
ip local-port .................................................................. 4068
ip source-violation .......................................................... 4069
tlifetime .................................................................... 4071
max-retransmissions ......................................................... 4072
mobile-ip foreign-agent context ....................................... 4073
msid length .................................................................. 4074
nai-construction ............................................................... 4075
new-call conflict ............................................................. 4076
pcf-monitor .................................................................. 4077
pcf-session-id-change restart-ppp ..................................... 4079
psdn type0-tft attempt-inner-match .................................. 4080
peer-pcf ........................................................................ 4081
policy ............................................................................ 4082
ppp ............................................................................... 4085
qos-profile-id-mapping .................................................... 4087
qos update .................................................................. 4089
registration-accept .......................................................... 4090
registration-ack-denied terminate-session-on-error .......... 4091
registration-deny ............................................................ 4092
registration-discard ........................................................ 4094
registration-update ........................................................ 4096
retransmission-timeout .................................................... 4097
sd-b-indication ............................................................... 4098
service-option ............................................................... 4100
setup-timeout ............................................................... 4102
simple-ip allow .............................................................. 4103
spi .............................................................................. 4104
spi zone ....................................................................... 4107
threshold a11-rtp-failure .................................................. 4108
threshold a11-rq-mg-discard ............................................ 4110
tft-validation wait-timeout ............................................... 4112
threshold all-rac-msg-discard .......................................................... 4113
threshold all-ppp-send-discard ....................................................... 4115
threshold init-req-rcvd-rate .......................................................... 4117

**PDSN Service RoHC Configuration Mode Commands** ........................ 4119
   cid-mode ...................................................................................... 4121
   end .......................................................................................... 4122
   exit .......................................................................................... 4123
   mru .......................................................................................... 4124
   profile ....................................................................................... 4125

**Peer-Server Configuration Mode Commands** .................................... 4127
   end .......................................................................................... 4128
   exit .......................................................................................... 4129
   mode ......................................................................................... 4130
   name .......................................................................................... 4131
   psp ............................................................................................ 4132
   routing-context ........................................................................... 4133
   self-point-code ......................................................................... 4134

**P-GW Service Configuration Mode Commands** ................................ 4135
   associate .................................................................................... 4136
   authorize-with-hss ...................................................................... 4138
   dns-client context ....................................................................... 4139
   end .......................................................................................... 4140
   exit .......................................................................................... 4141
   fqdn .......................................................................................... 4142
   gx-ll context ............................................................................... 4143
   newcall ...................................................................................... 4144
   pimn id ....................................................................................... 4145
   session-delete-delay .................................................................. 4146

**Policy Control Configuration Mode Commands** .............................. 4147
   apn-name-to-be-included .......................................................... 4148
   custom-reauth-trigger ................................................................ 4149
   diameter dictionary ................................................................... 4151
   diameter host-select reselect ..................................................... 4153
   diameter host-select row-precedence ....................................... 4155
   diameter host-select table .......................................................... 4158
   diameter origin endpoint ............................................................ 4160
   diameter request-timeout ............................................................ 4161
   end .......................................................................................... 4162
   exit .......................................................................................... 4163
   li-secret ..................................................................................... 4164
   failure-handling ....................................................................... 4165
   reauth-trigger ............................................................................ 4168

**PVC Configuration Mode Commands** ............................................ 4171
   bind .......................................................................................... 4172
   encapsulation aal5 ................................................................. 4174
   end .......................................................................................... 4175
   exit .......................................................................................... 4176
   shaping ...................................................................................... 4177
   shutdown ................................................................................. 4179

**PVC Interface Configuration Mode Commands** .............................. 4181
   description .................................................................................. 4182
   end .......................................................................................... 4183
exit
ip
ip access-group
ip address
ip mtu
ip ospf authentication-key
ip ospf authentication-type
ip ospf cost
ip ospf dead-interval
ip ospf hello-interval
ip ospf message-digest-key
ip ospf network
ip ospf priority
ip ospf retransmit-interval
ip ospf transmit-delay
QCI - QoS Mapping Configuration Mode Commands ........................................ 4201
end
exit
qci
QCI - RAN ID Mapping Configuration Mode Commands .................................. 4207
end
exit
profile-id
Radio Network Controller (RNC) Configuration Mode Commands .......... 4213
associate-gtpu-bind-address
description
direct-tunnel
end
exit
lac
overload-action disable
paging-non-searching-indication
pointcode
rab-modify-procedure
ranap paging-cause-ie
ranap signalling-indication-ie
release-compliance
reset-resource
Remote Address List Configuration Mode Commands ............................ 4231
address
end
exit
RoHC Profile Common Options Configuration Mode Commands .............. 4235
delay-release-hc-context-timer
end
exit
inactive-traffic-release-hc-context-timer
RoHC Profile Compression Configuration Mode Commands .................. 4241
delay-release-hc-context-timer
context-timeout
exit
ipid-history-size
RoHC Profile Configuration Mode Commands .......................... 4271
  common-options ........................................... 4272
  compression-options .................................... 4273
  decompression-options .................................. 4274
  end ..................................................... 4275
  exit ..................................................... 4276
RoHC Profile Decompression Configuration Mode Commands .......... 4277
  accept-delayed-pkts .................................... 4278
  context-timeout ....................................... 4279
  crc-errors-fo ......................................... 4280
  crc-errors-so ......................................... 4281
  end ..................................................... 4282
  exit ..................................................... 4283
  nack-limit ............................................. 4284
  optimistic-mode-ack ................................... 4285
  optimistic-mode-ack-limit ............................. 4286
  piggyback-wait-time ................................... 4287
  preferred-feedback-mode ................................ 4288
  rtp-sn ................................................. 4289
  rtp-sn-p ............................................... 4290
  sliding-window-ts .................................... 4291
  use-clock-option ...................................... 4292
  use-crc-option ........................................ 4293
  use-feedback .......................................... 4294
  use-jitter-option ..................................... 4295
  use-reject-option ..................................... 4296
  use-sn-not-valid-option ............................... 4297
  use-sn-option ......................................... 4298
Route-map Configuration Mode Commands ................................. 4299
end .................................................................................................................. 4300
exit..................................................................................................................... 4301
match as-path .................................................................................................. 4302
match interface ............................................................................................... 4303
match ip address .............................................................................................. 4304
match ip next-hop ............................................................................................ 4305
match metric ..................................................................................................... 4306
match origin ...................................................................................................... 4307
match route-type external .............................................................................. 4308
match tag .......................................................................................................... 4309
set as-path ........................................................................................................ 4310
set ip next-hop ................................................................................................. 4311
set metric .......................................................................................................... 4312
set metric-type .................................................................................................. 4313
set origin ........................................................................................................... 4314
set tag ................................................................................................................. 4315
set weight ......................................................................................................... 4316

RS-232 Port Configuration Mode Commands ............................................... 4317
  default ............................................................................................................. 4318
  end .................................................................................................................... 4319
  exit ................................................................................................................. 4320
  preferred slot .................................................................................................. 4321
  snmp trap link-status ..................................................................................... 4322
  terminal .......................................................................................................... 4323

Rulebase Configuration Mode Commands ..................................................... 4325
  action priority ................................................................................................. 4326
  bandwidth default-policy ................................................................................ 4329
  billing-records ............................................................................................... 4330
  cca diameter requested-service-unit .............................................................. 4332
  cca quota ........................................................................................................ 4334
  cca quota time-duration algorithm ................................................................. 4336
  cca radius accounting .................................................................................... 4338
  cca radius charging ....................................................................................... 4339
  cca radius user-password .............................................................................. 4340
  charging-rule-optimization .......................................................................... 4341
  constituent-policies ....................................................................................... 4342
  content-filtering category policy-id ............................................................... 4344
  content-filtering flow-any-error .................................................................... 4345
  content-filtering mode ................................................................................... 4346
  dynamic-rule ................................................................................................. 4348
  egcdr inactivity-meter ................................................................................... 4349
  egcdr inactivity-meter ................................................................................... 4350
  egcdr service-data-flow ............................................................................... 4351
  egcdr tariff .................................................................................................... 4352
  egcdr threshold .............................................................................................. 4353
  egcdr time-duration algorithm .................................................................... 4354
  end ................................................................................................................. 4355
  exit ................................................................................................................. 4356
  extract-host-from-uri .................................................................................... 4357
  fair-usage ...................................................................................................... 4358
  firewall dos-protection .................................................................................. 4359
  firewall flooding ............................................................................................ 4360
  firewall icmp-destination-unreachable-message-threshold ......................... 4361
  firewall icmp-destination-unreachable-message-threshold ......................... 4362
  firewall icmp-destination-unreachable-message-threshold ......................... 4363
  firewall icmp-destination-unreachable-message-threshold ......................... 4364
  firewall icmp-destination-unreachable-message-threshold ......................... 4365
  firewall icmp-destination-unreachable-message-threshold ......................... 4366
  firewall icmp-destination-unreachable-message-threshold ......................... 4367
firewall max-ip-packet-size ........................................ 4370
firewall mime-flood .................................................. 4371
firewall no-ruledef-matches ....................................... 4373
firewall policy ........................................................ 4375
firewall priority ....................................................... 4376
firewall tcp-first-packet-non-syn ................................. 4379
firewall tcp-idle-timeout-action ................................. 4380
firewall tcp-reset-message-threshold ............................ 4381
firewall tcp-syn-flood-intercept .................................. 4382
flow any-error ...................................................... 4384
flow control-handshaking ......................................... 4386
flow end-condition .................................................. 4388
flow limit-across-applications .................................... 4390
fw-and-nat default-policy ........................................ 4392
ip reassembly-timeout ............................................ 4393
ip reset-tos .......................................................... 4394
nat binding-record .................................................. 4395
nat policy ............................................................. 4397
nat suppress-aaa-update .......................................... 4399
p2p dynamic-flow-detection ....................................... 4400
post-processing priority ........................................... 4401
post-processing dynamic .......................................... 4403
qos-renegotiate timeout ........................................... 4405
radius threshold .................................................... 4406
route priority ........................................................ 4407
rtp dynamic-flow-detection ....................................... 4410
ruledef-parsing ...................................................... 4411
tcp 2msl-timeout ................................................... 4412
tcp check-window-size ............................................ 4413
tcp mss ............................................................... 4414
tcp out-of-order-timeout .......................................... 4416
tcp packets-out-of-order ......................................... 4417
timestamp rounding .................................................. 4418
transport-layer-checksum .......................................... 4420
udr threshold ........................................................ 4421
udr trigger ............................................................ 4423
url-blacklisting action ............................................ 4424
url-preprocessing ................................................... 4426
wtp out-of-order-timeout .......................................... 4427
wtp packets-out-of-order ......................................... 4428
xheader-encryption .................................................. 4430

**Ruledef Configuration Mode Commands** ........................................ 4431

  bearer ............................................................... 4432
  bearer 3gpp apn .................................................. 4433
  bearer 3gpp imsi .................................................. 4435
  bearer 3gpp rat-type ............................................ 4437
  bearer 3gpp sgsn-address ....................................... 4438
  bearer 3gpp2 bsid ............................................... 4439
  bearer 3gpp2 service-option .................................... 4441
  bearer apn ........................................................ 4442
  bearer imsi ........................................................ 4444
  bearer rat-type .................................................. 4446
  bearer sgsn-address ............................................. 4447
  bearer traffic-group ............................................ 4448
eca ................................................................. 4449
cca quota-state ................................................................. 4450
cca redirect-indicator ....................................................... 4451
copy-packet-to-log ........................................................... 4452
dns ................................................................................. 4454
dns answer-name ............................................................... 4455
dns any-match ................................................................. 4457
dns previous-state ............................................................. 4458
dns query-name ................................................................. 4459
dns return-code ............................................................... 4461
dns state .......................................................................... 4462
dns tid .............................................................................. 4463
e-mail ............................................................................. 4464
e-nd ................................................................................. 4466
exit ................................................................................ 4467
file-transfer ................................................................. 4468
file-transfer any-match ...................................................... 4469
file-transfer chunk-number ................................................ 4470
file-transfer current-chunk-length ....................................... 4471
file-transfer declared-chunk-length ................................... 4472
file-transfer declared-file-size ......................................... 4473
file-transfer filename ...................................................... 4474
file-transfer previous-state ............................................. 4476
file-transfer state .......................................................... 4477
file-transfer transferred-file-size ...................................... 4479
ftp .............................................................................. 4480
ftp any-match ................................................................. 4481
ftp client-ip-address ....................................................... 4482
ftp client-port ............................................................... 4483
ftp command args .......................................................... 4484
ftp command id .............................................................. 4486
ftp command name ........................................................ 4487
ftp connection-type ........................................................ 4489
ftp data-any-match ........................................................ 4490
ftp filename ................................................................. 4491
ftp pdu-length ............................................................... 4493
ftp pdu-type ................................................................. 4494
ftp previous-state .......................................................... 4495
ftp reply code ............................................................... 4496
ftp server-ip-address ...................................................... 4497
ftp server-port ............................................................. 4498
ftp session-length .......................................................... 4499
ftp state ................................................................. 4500
ftp url ........................................................................ 4502
ftp user ................................................................. 4503
http .............................................................................. 4504
http attribute-in-data ...................................................... 4506
http attribute-in-url ...................................................... 4507
http any-match ............................................................... 4508
http content disposition .................................................. 4509
http content-length .......................................................... 4510
http content-type ........................................................... 4512
http error ................................................................. 4513
http first-request-packet ................................................... 4515
http header-length .......................................................... 4516
http host ................................................................. 4518
http payload-length .......................................................... 4520
rtsp date .......................................................... 4681
rtsp previous-state ............................................ 4683
rtsp reply code .................................................. 4684
rtsp request method ............................................. 4685
rtsp request packet ............................................ 4687
rtsp rtsp-seq .................................................... 4688
rtsp rtsp-time .................................................. 4689
rtsp rtsp-uri ................................................... 4690
rtsp session-id .................................................. 4692
rtsp session-length ............................................ 4694
rtsp state ......................................................... 4695
rtsp uri .......................................................... 4696
rtsp uri sub-part ............................................... 4698
rtsp user-agent ................................................... 4700
rule-application ................................................. 4702
sdp .............................................................. 4703
sdp any-match ..................................................... 4704
sdp connection-ip-address ....................................... 4705
sdp media-audio-port ........................................... 4706
sdp media-video-port ............................................ 4707
sdp uplink ........................................................ 4708
secure-http ...................................................... 4709
secure-http any-match ........................................ 4710
secure-http uplink .............................................. 4711
sip .............................................................. 4712
sip any-match ....................................................... 4713
sip call-id .......................................................... 4714
sip content length ............................................... 4716
sip content type .................................................. 4717
sip from ............................................................ 4719
sip previous-state ............................................... 4721
sip reply code ..................................................... 4722
sip request method .............................................. 4723
sip request packet ................................................ 4724
sip state ............................................................ 4725
sip to ............................................................... 4726
sip uri ............................................................. 4728
smtp .............................................................. 4730
smtp any-match ..................................................... 4731
smtp command arguments ....................................... 4732
smtp command id .................................................. 4734
smtp command name ........................................... 4735
smtp mail-size .................................................... 4737
smtp pdu-length .................................................. 4739
smtp previous-state ............................................ 4741
smtp recipient ..................................................... 4742
smtp reply arguments ........................................... 4744
smtp reply id ..................................................... 4746
smtp reply status ................................................ 4747
smtp sender ........................................................ 4748
smtp session-length ............................................. 4750
smtp state .......................................................... 4752
tcp .............................................................. 4753
tcp analyzed out-of-order ....................................... 4754
tcp any-match ..................................................... 4756
tcp connection-initiator ......................................... 4757
www any-match ................................................................. 4830
www content type ............................................................. 4831
www downlink .................................................................. 4833
www first-request-packet .................................................. 4834
www header-length ............................................................ 4835
www host ........................................................................... 4836
www payload-length ........................................................... 4838
www pdu-length ................................................................. 4839
www previous-state ............................................................ 4840
www reply code ................................................................. 4841
www state .......................................................................... 4842
www transfer-encoding ....................................................... 4843
www url ............................................................................. 4845

SCCP Network Configuration Mode Commands .................. 4847
associate ......................................................................... 4848
description ....................................................................... 4849
destination ........................................................................ 4850
end .................................................................................. 4852
exit .................................................................................. 4853
global-title-translation ...................................................... 4854
hop-count ........................................................................ 4855
self-point-code .................................................................. 4856
timeout ............................................................................ 4857

Service Redundancy Protocol Configuration Mode Commands ... 4859
bind address ...................................................................... 4860
chassis-mode .................................................................... 4861
checkpoint session duration ............................................... 4862
configuration-interval ....................................................... 4863
dead-interval .................................................................... 4864
delay-interval ................................................................. 4865
end .................................................................................. 4866
exit .................................................................................. 4867
hello-interval .................................................................... 4868
monitor authentication probe ............................................. 4869
monitor bgp ....................................................................... 4870
peer-ip-address .................................................................. 4871
priority ............................................................................ 4872
route-modifier ................................................................... 4873

SGSN APN Policy Configuration Mode Commands ............... 4875
address-resolution-mode .................................................... 4876
cr ...................................................................................... 4877
direct-tunnel ................................................................. 4879
end .................................................................................. 4880
exit .................................................................................. 4881
gateway-address ............................................................ 4882
gtp ..................................................................................... 4884
ip ...................................................................................... 4886
pdp-data-inactivity .......................................................... 4889
qos class ........................................................................... 4891
qos prefer-as-cap ............................................................ 4894
qos rate-limit direction ..................................................... 4896
ranap allocation-retention-priority-ie ................................ 4900
restrict access-type .......................................................... 4903
SGSN ASP Configuration Mode Commands ........................................... 4905
  end ......................................................................................... 4906
  end-point .............................................................................. 4907
  exit ....................................................................................... 4909

SGSN Operator Policy Configuration Mode Commands .................. 4911
  accounting context ............................................................... 4913
  allocate-ptmsi-signature ..................................................... 4914
  apn ....................................................................................... 4915
  apn-restriction ...................................................................... 4916
  apn-selection-default .......................................................... 4917
  attach .................................................................................. 4918
  authenticate ........................................................................... 4922
  cc ......................................................................................... 4925
  charging context ................................................................. 4927
  description .......................................................................... 4928
  direct-tunnel ......................................................................... 4929
  dns-ggsn .............................................................................. 4930
  dns-bsgn .............................................................................. 4931
  encryption-algorithm-ums .................................................... 4932
  end ....................................................................................... 4933
  equivalent-plmn ................................................................. 4934
  exit ....................................................................................... 4935
  gmm information-in-messages ............................................ 4936
  gmm retrieve-equipment-identity ......................................... 4938
  gs-service ............................................................................. 4940
  gtp send .............................................................................. 4941
  gtpu fast-path ...................................................................... 4943
  integrity-algorithm-ums ....................................................... 4944
  location-area-list ............................................................... 4945
  map ....................................................................................... 4947
  map-service ......................................................................... 4948
  max-attached-subscribers ................................................... 4949
  mcc ....................................................................................... 4950
  network-initiated-pdp-activation ......................................... 4952
  nri ......................................................................................... 4953
  pdp-activate access-type ..................................................... 4954
  pdp-activate allow ............................................................... 4956
  pdp-activate restrict ............................................................ 4957
  ptmsi-reallocate ................................................................. 4959
  rau-inter .............................................................................. 4961
  rau-intra .............................................................................. 4964
  re-authenticate .................................................................... 4967
  reuse-authentication-triplets ............................................... 4968
  sgsn-address ....................................................................... 4969
  sgsn-number ...................................................................... 4970
  sgtp-service ........................................................................ 4971
  sms-mo ................................................................................. 4972
  sms-mt .................................................................................. 4973
  srns-inter ............................................................................. 4974
  srns-intra ............................................................................. 4975
  subscriber-control-inactivity ................................................ 4976
  super-charger ...................................................................... 4977
  wildcard-apn ...................................................................... 4978
  zone-code ............................................................................ 4979
SGSN Pool Area Configuration Mode Commands................................. 4981
end................................................................. 4983
exit................................................................. 4984
hash-value .................................................. 4985
lac............................................................... 4987
SGSN PSP Configuration Mode Commands............................................ 4989
associate ..................................................... 4990
end............................................................... 4991
disable/enable super-accounting .................................................. 4993
exit............................................................... 4994
psp-mode ...................................................... 4995
routing-context ............................................. 4996
sctp............................................................... 4997
sctp-alpha .................................................... 4998
sctp-beta ....................................................... 4999
sctp-checksum-type ......................................... 5000
sctp-cookie-life ............................................. 5001
sctp-max-assoc-retx ......................................... 5002
sctp-max-init-retx ........................................... 5003
sctp-max-mtu-size ........................................... 5004
sctp-max-out-strm .......................................... 5005
sctp-max-path-retx ........................................... 5006
sctp-linux .................................................... 5007
sctp-rto-max .................................................. 5008
sctp-rto-min .................................................. 5009
sctp-sack-frequency ......................................... 5010
sctp-sack-period ............................................ 5011
timeout ....................................................... 5012
SGSN Service Configuration Mode Commands................................. 5013
accounting ................................................... 5014
cc profile ..................................................... 5016
core-network ............................................... 5018
disable/enable super-charger ......................................... 5019
dns-israu-mcc-mnc-encoding ................................ 5020
end............................................................... 5021
gmm ........................................................... 5022
exit............................................................... 5023
lte-gsm ........................................................ 5024
max-pdp-contexts ........................................... 5025
mobile-application-part ......................................... 5026
network-sharing cs-ps-coordination ....................................... 5027
nri-length ..................................................... 5028
override-lac-li .............................................. 5029
override-rac-li .............................................. 5030
rac .............................................................. 5031
ran-protocol .................................................. 5032
sgsn-number .................................................. 5033
sgtp-service ................................................... 5034
sm .............................................................. 5035
SGTP Service Configuration Mode Commands................................. 5043
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>cscf session-template</td>
<td>5107</td>
</tr>
<tr>
<td>data-tunneling ignore df-bit</td>
<td>5108</td>
</tr>
<tr>
<td>dceca origin host</td>
<td>5109</td>
</tr>
<tr>
<td>dceca origin endpoint</td>
<td>5110</td>
</tr>
<tr>
<td>dceca peer-select</td>
<td>5111</td>
</tr>
<tr>
<td>default</td>
<td>5112</td>
</tr>
<tr>
<td>dns</td>
<td>5115</td>
</tr>
<tr>
<td>eap</td>
<td>5116</td>
</tr>
<tr>
<td>encrypted password</td>
<td>5117</td>
</tr>
<tr>
<td>end</td>
<td>5118</td>
</tr>
<tr>
<td>exit</td>
<td>5119</td>
</tr>
<tr>
<td>external-inline-server</td>
<td>5120</td>
</tr>
<tr>
<td>firewall policy</td>
<td>5121</td>
</tr>
<tr>
<td>fw-and-nat policy</td>
<td>5123</td>
</tr>
<tr>
<td>idle-timeout-activity</td>
<td>5124</td>
</tr>
<tr>
<td>ims application-manager</td>
<td>5125</td>
</tr>
<tr>
<td>ims-auth-service</td>
<td>5126</td>
</tr>
<tr>
<td>inter-psdn-handoff</td>
<td>5127</td>
</tr>
<tr>
<td>ip access-group</td>
<td>5128</td>
</tr>
<tr>
<td>ip address</td>
<td>5129</td>
</tr>
<tr>
<td>ip address pool</td>
<td>5130</td>
</tr>
<tr>
<td>ip address secondary-pool</td>
<td>5131</td>
</tr>
<tr>
<td>ip allowed-dscp</td>
<td>5132</td>
</tr>
<tr>
<td>ip context-name</td>
<td>5135</td>
</tr>
<tr>
<td>ip header-compression</td>
<td>5136</td>
</tr>
<tr>
<td>ip hide-service-address</td>
<td>5139</td>
</tr>
<tr>
<td>ip local-address</td>
<td>5140</td>
</tr>
<tr>
<td>ip multicast discard</td>
<td>5141</td>
</tr>
<tr>
<td>ip qos-dscp</td>
<td>5142</td>
</tr>
<tr>
<td>ip route</td>
<td>5144</td>
</tr>
<tr>
<td>ip source-validation</td>
<td>5145</td>
</tr>
<tr>
<td>ip user-datagram-tos copy</td>
<td>5146</td>
</tr>
<tr>
<td>ip vlan</td>
<td>5147</td>
</tr>
<tr>
<td>ipv6 access-group</td>
<td>5148</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>5149</td>
</tr>
<tr>
<td>ipv6 dns</td>
<td>5150</td>
</tr>
<tr>
<td>ipv6 dns-proxy</td>
<td>5151</td>
</tr>
<tr>
<td>ipv6 egress-address-filtering</td>
<td>5152</td>
</tr>
<tr>
<td>ipv6 initial-router-advt</td>
<td>5153</td>
</tr>
<tr>
<td>ipv6 interface-id</td>
<td>5154</td>
</tr>
<tr>
<td>ipv6 minimum-link-mtu</td>
<td>5155</td>
</tr>
<tr>
<td>ipv6 secondary-address</td>
<td>5156</td>
</tr>
<tr>
<td>l2tp send accounting-correlation-info</td>
<td>5157</td>
</tr>
<tr>
<td>l3-to-l2-tunnel address-policy</td>
<td>5158</td>
</tr>
<tr>
<td>loadbalance-tunnel-peers</td>
<td>5159</td>
</tr>
<tr>
<td>long-duration-action</td>
<td>5160</td>
</tr>
<tr>
<td>mobile-ip</td>
<td>5162</td>
</tr>
<tr>
<td>mobile-ip ha</td>
<td>5165</td>
</tr>
<tr>
<td>mobile-ip reg-lifetime-override</td>
<td>5166</td>
</tr>
<tr>
<td>mobile-ip send accounting-correlation-info</td>
<td>5167</td>
</tr>
<tr>
<td>mobile-ipv6</td>
<td>5168</td>
</tr>
<tr>
<td>nai-construction-domain</td>
<td>5169</td>
</tr>
<tr>
<td>nbns</td>
<td>5170</td>
</tr>
<tr>
<td>nexthop-forwarding-address</td>
<td>5171</td>
</tr>
<tr>
<td>npu qos</td>
<td>5172</td>
</tr>
<tr>
<td>nw-reachability-server</td>
<td>5174</td>
</tr>
<tr>
<td><strong>class-map</strong></td>
<td>5245</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>end</strong></td>
<td>5246</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>5247</td>
</tr>
<tr>
<td><strong>flow-tp-trigger</strong></td>
<td>5248</td>
</tr>
<tr>
<td><strong>ip header-compression</strong></td>
<td>5249</td>
</tr>
<tr>
<td><strong>qos encaps-header</strong></td>
<td>5250</td>
</tr>
<tr>
<td><strong>qos traffic-police</strong></td>
<td>5251</td>
</tr>
<tr>
<td><strong>qos user-datagram dscp-marking</strong></td>
<td>5253</td>
</tr>
<tr>
<td><strong>sess-tp-trigger</strong></td>
<td>5254</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>5255</td>
</tr>
</tbody>
</table>

**Tunnel Interface Configuration Mode Commands** ............................ 5257

- **description** ........................................................................... 5258
- **end** ..................................................................................... 5259
- **exit** .................................................................................... 5260
- **ip address** .......................................................................... 5261
- **ipv6 address** ....................................................................... 5262
- **tunnel-mode** ......................................................................... 5263

**UDR Format Configuration Mode Commands** ................................. 5265

- **attribute** ............................................................................. 5266
- **end** ..................................................................................... 5271
- **event-label** ......................................................................... 5272
- **exit** .................................................................................... 5273
- **rule-variable** ....................................................................... 5274

**UDR Module Configuration Mode Commands** ................................. 5277

- **cdr** ...................................................................................... 5278
- **end** ..................................................................................... 5281
- **exit** .................................................................................... 5282
- **file** ..................................................................................... 5283

**VLAN Configuration Mode Commands** ......................................... 5289

- **bind interface** ..................................................................... 5290
- **end** ..................................................................................... 5291
- **exit** .................................................................................... 5292
- **ingress-mode** ....................................................................... 5293
- **shutdown** ............................................................................ 5294
- **vlan-map** ............................................................................. 5295

**x-header Format Configuration Mode Commands** ........................... 5297

- **end** ..................................................................................... 5298
- **exit** .................................................................................... 5299
- **insert** .................................................................................. 5300
About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.
Conventions Used

The following tables describe the conventions used throughout this documentation.

### Icon

<table>
<thead>
<tr>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
<tr>
<td>Electro-Static Discharge (ESD)</td>
<td>Alerts you to take proper grounding precautions before handling a product.</td>
</tr>
</tbody>
</table>

### Typeface Conventions

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

### Command Syntax Conventions

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>{ keyword or variable}</strong></td>
</tr>
<tr>
<td>Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.</td>
</tr>
</tbody>
</table>
## Conventions Used

<table>
<thead>
<tr>
<th>Command Syntax Conventions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[keyword or variable]</code></td>
<td>Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
</tbody>
</table>
Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.
Chapter 1
Command Line Interface Overview

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

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

This section provides the following information about the CLI:

- CLI Structure
- CLI Command Modes
- CLI Administrative Users
- CLI Contexts
- Understanding the CLI Command Prompt
- CLI Command Syntax
- Entering and Viewing CLI Commands
- Obtaining CLI Help
- Exiting the CLI and CLI Command Modes
- Accessing the CLI
CLI Structure

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

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

There are two primary CLI command modes:

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

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

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

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

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

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

Administrative User Types

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

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

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

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

Authenticating Administrative Users with RADIUS

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

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

The default permission is none (0), meaning that service is refused even if properly authenticated via RADIUS.

RADIUS Mapping System

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
</table>

Table 1. RADIUS Attribute/Value Mapping System
### Attribute Values

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login (Operator)</td>
<td>1</td>
</tr>
<tr>
<td>Framed</td>
<td>2</td>
</tr>
<tr>
<td>Callback_Login</td>
<td>3</td>
</tr>
<tr>
<td>Callback_Framed</td>
<td>4</td>
</tr>
<tr>
<td>Outbound</td>
<td>5</td>
</tr>
<tr>
<td>Administrative (Administrator)</td>
<td>6</td>
</tr>
<tr>
<td>NAS_Prompt</td>
<td>7</td>
</tr>
<tr>
<td>Authenticate_Only</td>
<td>8</td>
</tr>
<tr>
<td>Callback_NAS_Prompt</td>
<td>9</td>
</tr>
<tr>
<td>Call_Check</td>
<td>10</td>
</tr>
<tr>
<td>Callback_Administrative</td>
<td>11</td>
</tr>
<tr>
<td>Voice</td>
<td>12</td>
</tr>
<tr>
<td>Fax</td>
<td>13</td>
</tr>
<tr>
<td>Modem_Relay</td>
<td>14</td>
</tr>
<tr>
<td>IAPP_Register</td>
<td>15</td>
</tr>
<tr>
<td>IAPP_AP_Check</td>
<td>16</td>
</tr>
<tr>
<td>Authorize_Only</td>
<td>17</td>
</tr>
<tr>
<td>Inspector</td>
<td></td>
</tr>
<tr>
<td>Security_Admin</td>
<td></td>
</tr>
</tbody>
</table>

### RADIUS Privileges

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

**Table 2. CLI Privilege Roles and RADIUS Service Types**

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

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

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

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

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

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

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

![Figure 1. User Privileges](image)

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

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

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

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

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

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

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

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

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

**Allowed Commands per User Type**

With the exception of security administrators, all other management users are limited to a subset of the entire command list as described in the *Command Line Interface Reference*. This section defines the commands allowed for each management user type. As stated previously, inspectors and operators are limited to only a subset of the Exec Mode commands.
Inspector Mode Commands

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

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

Operator Mode Commands

In the Exec mode, system operators can access all inspector mode commands plus the following commands:

- aaa test
- alarm cutoff
- bulkstats force
- card
- clear (a subset of all clear command variations)
- debug
- dhcp test
- gtpc test
- gtppp interim
- gtppp test
- gtpu test
- gtpv0 test
- host
- logging active
- logging filter
- logging trace
- newcall
- no card
- no debug
- no newcall policy
- port
- ppp echo-test
- radius interim accounting
- radius test
- rlogin
- show access-group
- show access-list
- show access-flow
- show access statistics
- show configuration
- show snmp transports
- ssh
- telnet
- test alarm

**Administrator Mode Commands**

Administrators can access all system commands except:

**Context Config Mode**

- config-administrator
- operator
• inspector
• administrator

Global Config Mode

• snmp community
• snmp user
• local-user
• suspend local-user

Exec Mode

• show snmp communities
• clear (all clear command variations)
• show local-user
• password change local-user

**Security Administrator Mode Commands**

Security administrators can access all system commands.
CLI Contexts

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

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

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

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

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

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

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

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

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

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

**Figure 2. CLI Command Prompt**

- **Context Pointer:** Shows the context in which the user is currently working.
- **System Host Name:** Shows the currently configured host name.
- **Command Mode:** Shows the specific command mode or sub-mode in which the user is currently working.
- **User Privilege Indicator:** Indicates the user mode.
  - `#` indicates administrator / config-administrator privileges
  - `>` indicates inspector / operator privileges only
CLI Command Syntax

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

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

**Example**

In the following example, *slot_number* is the command variable for the *info* keyword:

```
show slot info slot_number
```

*slot_number* is a variable representing a particular slot (1 through 48).
Entering and Viewing CLI Commands

This section describes various methods for entering commands into the CLI.

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

Entering Partial CLI Commands

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

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

Ambiguous Command

CLI Command Auto-completion

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

Example
```bash
[local]host_name# sho<Tab>
[local]host_name# show
```
If you do not enter enough characters to allow the CLI to determine the appropriate command to use, the CLI displays all commands that match the characters you entered with auto-completion:

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

[local]host_name#
```

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

Example
```bash
[local]host_name# sh?
show - Displays information based on a specified argument
```
Using CLI Auto-Pagination

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

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

`[local]host_name# show configuration | more`

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

Using CLI Autoconfirmation

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

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

**Example**

Saving a configuration:

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

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

**Examples**

You create context named “newcontext”:

```
[local]host_name(config)# context newcontext
Are you sure ? [Yes | No]: yes
[newcontext]host_name(config-ctx)#
```
You revisit the context named “newcontext”:

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

On another occasion, you misspell the context named “newcontext”:

[local]host_name(config)# context newcontext
Are you sure? [Yes | No]: n
Action aborted
[local]host_name(config)#

After aborting the above action, you can again revisit “newcontext”:

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

You can control CLI autoconfirmation at the following levels:

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

### Regulating the Command Output

For many CLI commands, you can use `| grep` and/or `| more` keywords to regulate or control the command’s output. Use the `| grep` keyword to filter through a command’s output for certain expressions or patterns. Only those portions of the output that contain or exclude the pattern are displayed. The `| grep` has the following syntax:

```
| grep [ -i | -v | --ignore-case | --invert-match ] expression
```

**Table 4. grep Keywords**

<table>
<thead>
<tr>
<th>Alternative Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>Specifies the filtering of the command’s output for a particular expression while ignoring case. Lower case matches the same as upper case.</td>
</tr>
<tr>
<td>-v</td>
<td>Specifies the filtering of the command’s output for everything excluding a particular expression.</td>
</tr>
<tr>
<td>--ignore-case</td>
<td>The long form of the -i option.</td>
</tr>
</tbody>
</table>
Alternative Keyword | Description
--- | ---
--invert-match | The long form of the -v option.
expression | Specifies the character pattern to find in the command’s output.

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

Viewing Command History

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

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

**Table 5. EMACS Shortcut Keystrokes**

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

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

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

  **Example**

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

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

  **Example**

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

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

  **Example**

  ```
  [local]host_name# show card info ?
  <Enter card number as an integer ranging 1 to 48> | - Pipeline <cr> - Carriage Return or <Enter> key
  ```
Exiting the CLI and CLI Command Modes

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

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

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

Exiting Configuration Sub-modes

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

**Example**

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

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

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

**Example**

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

Exiting Global Configuration Mode

To exit Global Configuration Mode, and return to the Exec Mode prompt, type the `exit` command at the prompt.
Ending a CLI Session

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

Access the CLI through the following methods:

- Local login through a Console port using the RS-232 serial cable supplied with the card
- Remote login using Telnet and Secure Shell (SSH) access to the CLI through any IP interface on the system.

**Important:** Even though you can access the CLI remotely through any available IP interface, it is recommended that management traffic be isolated from network traffic by using one of the SPIO card management interfaces. You can use remote login methods only after the system has been configured to support the various access methods.

**Important:** Multiple CLI sessions are supported, but the number of sessions is dependent on the amount of available memory. The Resource Manager reserves enough resources so that as a minimum, 15 CLI sessions are assured. One of the CLI sessions is always reserved for use exclusively by a CLI session on an SPIO console interface. Additional CLI sessions beyond the pre-reserved set are permitted if sufficient SMC resources are available. If the Resource Manager is unable to reserve additional resources, you are prompted whether to allow the system to create the new CLI session, even without the reserved resources.

### Accessing the CLI Locally Using the Console Port

This section provides instructions for accessing the CLI locally through the console port.
Access the console port with the RJ-45-to-DB-9 serial (EIA-232) cable that is shipped with the Switch Processor Input/Output (SPIO). Connect to a workstation that has a communications application that accesses the workstation’s serial port, such as Minicom for Linux or HyperTerminal® for Microsoft Windows®.

Each of the two SPIO Line Cards installed in the system provides a console port for accessing the CLI. The CLI is only accessible from the SPIO that is active—typically the SPIO installed in chassis slot 24.

For normal operation, the SMC in chassis slot 8 serves as the active processing card for the system. The SPIO that corresponds to this SMC is installed in slot 24. For the processing card in chassis slot 9, the corresponding SPIO is installed in slot 25.
**Important:** In the event of a SMC switchover, in which processes are switched from the processing card in slot 8 that was previously active to the redundant processing card in slot 9, the SPIO in slot 24 continues to serve as the active SPIO. Therefore, the console port is still accessible through that SPIO.

Follow the instructions below to connect to the console port.

1. Connect the RJ-45 end of the cable to the port labeled *Console*.
2. Connect the DB-9 end of the cable to the serial port on the workstation.
3. Configure the communications application to support the following:

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

**Important:** To change the configuration defined in the table above, modify the `terminal` command located in the Global configuration mode.

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

## Remotely Accessing the CLI

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

You can find examples of how to configure this in the *Getting Started* chapter.
Chapter 2
AAA Server Group Configuration Mode Commands

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

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

aaa group group_name

AAA Server Group Configuration Mode
```
diameter accounting

This command configures Diameter accounting parameters.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq | rf-plus } | endpoint endpoint_name | hd-mode fall-back-to-local | hd-storage-policy hd_policy | max-retries tries | max-transmissions transmissions | request-timeout duration | server host_name priority priority }

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

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

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

endpoint: Removes the configured accounting endpoint, and the default accounting server configured in the default AAA group will be used.

hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.

hd-storage-policy: Disables use of the specified HD storage policy.

max-retries: Disables the configured retry attempts for Diameter accounting in the current AAA group.

max-transmissions: Disables the configured maximum transmission attempts for Diameter accounting in the current AAA group.

server host_name: Removes the configured Diameter host host_name from this AAA server group for Diameter accounting.

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

dictionary: Sets the context's dictionary as the system default.

hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.

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

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

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


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

Specifies the Diameter accounting dictionary.

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

**nasreq**: nasreq dictionary—the dictionary defined by RFC 4005.

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

```
endpoint endpoint_name
```

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

**endpoint_name**: must be a string of 1 through 63 characters in length.

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

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

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

Associates the specified HD Storage policy with the AAA group.

**hd_policy**: must be the name of a configured HD Storage policy, and must be a string of 1 through 63 alpha and/or numeric characters in length.

HD Storage policies are configured through the Global Configuration Mode.

This and the **hd-mode** command are used to enable the storage of Rf Diameter Messages to HDD in case all Diameter Servers are down or unreachable.

```
max-retries tries
```

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

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

Default: 0

```
max-transmissions transmissions
```

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

**transmissions**: must be an integer from 1 through 1000.

Default: 0

```
request-timeout duration
```

Specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request.

**duration**: specifies the number of seconds, and must be an integer from 1 through 3600.

Default: 20

```
server host_name priority priority
```

Specifies the current context Diameter accounting server’s host name and priority.

**host_name**: specifies the Diameter host name, and must be a string of 1 through 63 characters in length.
priority specifies the relative priority of this Diameter host. The priority is used in server selection. The priority must be an integer from 1 through 1000.

Usage

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

Example

The following command configures the Diameter accounting dictionary:

```
diameter accounting dictionary <dictionary>
```

The following command configures the Diameter endpoint:

```
diameter accounting endpoint <endpoint_name>
```

The following commands configure Diameter accounting options:

```
diameter accounting max-retries <tries>
diameter accounting max-transmissions <transmissions>
diameter accounting request-timeout <duration>
diameter accounting server <host_name> priority <priority>
```

The following commands disable/clear the options:

```
no diameter accounting endpoint
no diameter accounting server <host_name>
```
diameter authentication

This command configures Diameter authentication parameters.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
diameter authentication { dictionary ( aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq ) | endpoint endpoint_name | max-retries tries | max-transmissions transmissions | redirect-host-avp { just-primary | primary-then-secondary } | request-timeout duration | server host_name priority priority }

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

no diameter authentication { endpoint | max-retries | max-transmissions | server host_name }
```

```
no diameter authentication { endpoint | max-retries | max-transmissions | server } host_name

dictionary: Sets the context’s dictionary as the system default.
endpoint: Removes the configured authentication endpoint, and the default server configured in default AAA group will be used.
max-retries: Disables the configured retry attempts for Diameter authentication in the current AAA group.
max-transmissions: Disables the configured maximum transmission attempts for Diameter authentication in the current AAA group.
server host_name: Removes the configured Diameter host host_name from this AAA server group for Diameter authentication.
```

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

```
max-retries: Sets the retry attempts for Diameter authentication requests in the current AAA group to default 0 (disable).
max-transmissions: Sets the configured maximum transmission attempts for Diameter authentication in the current AAA group to default 0 (disable).
redirect-host-avp: Sets the redirect choice to default (just-primary).
request-timeout: Sets the timeout duration, in seconds, for Diameter authentication requests in the current AAA group to default 20.
```

```
```

Cisco ASR 5000 Series Command Line Interface Reference
Specifies the Diameter authentication dictionary.

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

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

### nasreq

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

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

Default: 0

### max-transmissions

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

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

Default: 0

### diameter authentication redirect-host-avp { just-primary | primary-then-secondary }

Specifies whether to use just one returned AVP, or use the first returned AVP as selecting the primary host and the second returned AVP as selecting the secondary host.

**just-primary:** Redirect only to primary host.

**primary-then-secondary:** Redirect to primary host, if fails then redirect to the secondary host.

Default: just-primary

### request-timeout duration

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.

*duration* specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request, and must be an integer from 1 through 3600.

Default: 20 seconds

### server host-name priority priority

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

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

Example
The following command configures the Diameter authentication dictionary:

```
diameter authentication dictionary <dictionary>
```

The following command configures the Diameter endpoint:

```
diameter authentication endpoint <endpoint_name>
```

The following commands configure Diameter authentication options:

```
diameter authentication max-retries <tries>
diameter authentication max-transmissions <transmissions>
diameter authentication redirect-host-avp primary-then-secondary
diameter authentication server <host_name> priority <priority>
diameter authentication request-timeout <duration>
```

The following commands disable/clear the options:

```
no diameter authentication endpoint
no diameter authentication server <host_name>
```
diameter authentication failure-handling

This command configures the failure handling for Diameter authentication requests and Diameter EAP requests.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

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

do diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } result-code start_result_code [ to end_result_code ]

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

- **no**
  Disables Diameter authentication failure handling.

- **default**
  Configures the default Diameter authentication failure handling setting.

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

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

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

- **request-timeout action { continue | retry-and-terminate | terminate }**
  Specifies the action to be taken for failures:
  * **continue**: Continues session
  * **retry-and-terminate**: First retries, if it fails then terminates the session
  * **terminate**: Terminates session
result-code start_result_code [ to end_result_code ] action { continue | retry-and-terminate | terminate }

start_result_code: Specifies the result code number, must be an integer from 1 through 65535.
to end_result_code: Specifies the upper limit of a range of result codes. to end_result_code must be greater than start_result_code.

action { continue | retry-and-terminate | terminate }: Specifies action to be taken for failures:
  • continue: Continues
  • retry-and-terminate: First retries, if it fails then terminates
  • terminate: Terminates

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

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

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

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

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
```
end
```

Usage
Use this command to return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

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

This command associates the specific AAA group with a Virtual Routing and Forwarding (VRF) Context instance for GRE tunnel interface configuration. By default the VRF is NULL, which means that AAA group is associated with global routing table.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius ip vrf vrf_name

no radius ip vrf

no
Removes/disassociates configured IP Virtual Routing and Forwarding (VRF) context instance.

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

Usage
Use this command to associate/disassociate a pre-configured VRF context for a GRE tunnel interface. By default the VRF is NULL, which means that AAA group is associated with global routing table.

Example
The following command associates VRF context instance GRE_vrf1 with this AAA group:

radius ip vrf GRE_vrf1
radius

This command configures basic RADIUS options.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
radius { realtime minutes | detect-dead-server { consecutive-failures count | response-timeout seconds } | dictionary dictionary | max-outstanding messages | max-retries tries | max-transmissions transmissions | strip-domain { authentication-only | accounting-only } | timeout idle_seconds }

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

no radius { detect-dead-server | max-transmissions | strip-domain }
```

- **no**
  Removes configuration for the specified keyword.

- **default**
  Configures default setting for the specified keyword.

**dictionary dictionary**

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

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>customXX</td>
<td>These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. XX is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>3gpp</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.</td>
</tr>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>starent-vsa1</td>
<td>This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.</td>
</tr>
</tbody>
</table>
### Dictionary Description

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

---

**deadtime minutes**

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

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

**Important:** For a complete explanation of RADIUS server states, refer to the RADIUS Server State Behavior appendix in the AAA Interface Administration and Reference.

**detect-dead-server**

```plaintext
detect-dead-server { consecutive-failures count | keepalive | response-timeout seconds }
```

**consecutive-failures count**: Specifies the number of consecutive failures, for any AAA Manager, before a server’s state is changed from “Active” to “Down”. count must be an integer from 1 through 1000. Default: 4.

**keepalive**: Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default is disabled.

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

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

**Important:** The “Active” or “Down” state of a RADIUS server as defined by the system, is based on accessibility and connectivity. For example, if the server is functional but the system has placed it into a “Down” state, it could be the result of a connectivity problem. When a RADIUS server’s state is changed to “Down”, a trap is sent to the management station and the deadtime timer is started.
**max-outstanding messages**
Default: 256
Specifies the maximum number of outstanding messages a single AAA Manager instance will queue. 
messages must be an integer from 1 through 4000.

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

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

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

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

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

**Example**

```
radius detect-dead-server consecutive-failures 6
radius dictionary 3gpp2
radius timeout 300
```
radius strip-domain authentication-only
radius accounting

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius accounting { archive [ stop-only ] | deadtime minutes | detect-dead-server { consecutive-failures count | keepalive | response-timeout seconds } | interim interval seconds | max-outstanding messages | max-pdu-size octets | max-retries tries | max-transmissions transmissions | timeout idle_seconds }

default radius accounting { deadtime | detect-dead-server | max-outstanding | max-pdu-size | max-retries | max-transmissions | timeout }

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

---

no
Removes configuration for the specified keyword.

default
Configures the default setting for the specified keyword.

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

stop-only specifies archiving of only STOP accounting messages.

deadtime minutes
Default: 10 minutes
Specifies the number of minutes to wait before changing the state of a RADIUS server from “Down” to “Active”.

minutes must be an integer from 0 through 65535.

**Important:** This parameter should be set to allow enough time to remedy the issue that originally caused the server’s state to be changed to “Down”. After the deadtime timer expires, the system returns the server’s state to “Active” regardless of whether or not the issue has been fixed.
Important: For a complete explanation of RADIUS server states, refer to the RADIUS Server State Behavior Appendix in the AAA Interface Administration and Reference.

\begin{verbatim}
\texttt{detect-dead-server \{ consecutive-failures count | keepalive | response-timeout seconds \}}
\end{verbatim}

\texttt{consecutive-failures count}: Specifies the number of consecutive failures, for any AAA Manager, before a server’s state is changed from “Active” to “Down”. \texttt{count} must be an integer from 1 through 1000. Default: 4

\texttt{keepalive}: Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default: disabled

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

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

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

Important: For a complete explanation of RADIUS server states, refer to the RADIUS Server State Behavior Appendix in the AAA Interface Administration and Reference.

\begin{verbatim}
\texttt{interim interval seconds}
\end{verbatim}

Default: Disabled

Specifies the time interval, in seconds, for sending accounting INTERIM-UPDATE records. \texttt{seconds} must be an integer from 50 through 40000000.

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

\begin{verbatim}
\texttt{max-outstanding messages}
\end{verbatim}

Default: 256

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue. \texttt{messages} must be an integer from 1 through 4000.

\begin{verbatim}
\texttt{max-pdu-size octets}
\end{verbatim}

Default: 2048

Specifies the maximum sized packet data unit which can be accepted/generated, in bytes (octets). \texttt{octets} must be an integer from 512 through 2048.
max-retries tries
Default: 5
Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding” and the detect dead server consecutive failures count is incremented. tries must be an integer from 0 through 65535. Once the maximum number of retries is reached this is considered a single failure for the consecutive failures count for detecting dead servers.

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

timeout seconds
Default: 3
Specifies the amount of time to wait for a response from a RADIUS server before retransmitting a request. seconds must be an integer from 1 through 65535.

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

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

radius accounting timeout 16
radius accounting apn-to-be-included

This command specifies the APN name inclusion for RADIUS accounting.

Product
GGSN

Privilege
Security Administrator, Administrator

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

default radius accounting apn-to-be-included

default
Configures the default setting.

gi
Specifies the use of Gi APN name in RADIUS accounting request. Gi APN represents the APN received in the Create PDP context request message from SGSN.

gn
Specifies the use of Gn APN name in RADIUS accounting request. Gn APN represents the APN selected by the GGSN.

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

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

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

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

default radius accounting algorithm
```

**default**
ConFigures the default setting.
Default: `first-server`

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

`n` is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128.

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

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

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

**Example**
The following command configures to use the round-robin algorithm for RADIUS accounting server selection:
radius accounting algorithm round-robin
radius accounting billing-version

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius accounting billing-version version

default radius accounting billing-version

default
Configures the default setting.
Default: 0

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

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

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

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

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

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

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

```
default radius accounting gtp trigger-policy
```

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

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

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

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

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

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

```
default radius accounting gtp trigger-policy
```
radius accounting ha policy

Configures the RADIUS accounting policy for HA sessions.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

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

default
Configures the default setting.

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

custom1-aaa-res-mgmt
Accounting Start/Stop messages are generated to assist special resource management done by AAA servers. It is similar to the session-start-stop accounting policy, except for the following differences:
- Accounting Start is also generated during MIP session handoffs.
- No Accounting stop is generated when an existing session is overwritten and the new session continues to use the IP address assigned for the old session.
- Accounting Start is generated when a new call overwrites an existing session.

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

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

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

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

**Product**

GGSN, PDSN, HA, HSGW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
radius accounting interim { interval seconds | volume { downlink bytes uplink bytes | total bytes | uplink bytes downlink bytes } }

no radius accounting interim volume
```

- **no**
  
  Disables RADIUS interim accounting.

- **interval seconds**

  Specifies the time interval, in seconds, between sending interim accounting records. `seconds` must be an integer from 50 through 40,000,000.

- **volume { downlink bytes uplink bytes | total bytes | uplink bytes downlink bytes }**

  - **downlink bytes**
    
    Specifies the downlink to uplink volume limit, in bytes, for RADIUS Interim accounting. `bytes` must be an integer from 100,000 through 4,000,000,000.

  - **total bytes**
    
    Specifies the total volume limit, in bytes, for RADIUS interim accounting. `bytes` must be an integer from 100,000 through 4,000,000,000.

  - **uplink bytes**
    
    Specifies the uplink to downlink volume limit, in bytes, for RADIUS interim accounting. `bytes` must be an integer from 100,000 through 4,000,000,000.

**Usage**

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

**Example**

The following command triggers RADIUS interim accounting when the total volume of uplink and downlink bytes reaches 110000:

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

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

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

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

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

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

- **no**
  - Removes configuration for the specified keyword.

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

- **list list_id**
  - Enters the Remote Address List Configuration mode. This mode configures a list of remote addresses that can be referenced by the subscriber’s profile.

  - `list_id` must be an integer from 1 through 65535.

**Usage**

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

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

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

**Example**

```
radius accounting ip remote-address collection
```
radius accounting keepalive

Configures the keepalive authentication parameters for the RADIUS accounting server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | default ] radius accounting keepalive { calling-station-id id | consecutive-response number | framed-ip-address ip_address | interval seconds | retries number | timeout seconds | username name }
```

---

**no**
Removes configuration for the specified keyword.

**default**
Configures the default setting for the specified keyword.

**calling-station-id id**
Configures the Calling-Station-Id to be used for the keepalive authentication.
`id` must be an alpha and/or numeric string of 1 through 15 characters in length.
Default: 000000000000000

**consecutive-response number**
Configures the number of consecutive authentication response after which the server is marked as reachable.
`number` must be an integer from 1 through 10.
Default: 1

**framed-ip-address ip_address**
Configures the framed-ip-address to be used for the keepalive accounting.
`ip_address` must be specified using the standard IPv4 dotted decimal notation.

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

**retries number**
Configures the number of times the keepalive access request to be sent before marking the server as unreachable.
`number` must be an integer from 3 through 10.
Default: 3
timeout seconds
Configures the time interval between each keepalive access request retries.
seconds must be an integer from 1 through 30.
Default: 3 seconds

username name
Configures the user name to be used for authentication.
name must be an alpha and/or numeric string of 1 through 127 characters in length.
Default: Test-Username

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

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

    radius accounting keepalive username Test-Username2

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

    radius accounting keepalive retries 4
radius accounting pdif trigger-policy

Configures the policy for generating START/STOP pairs in overflow condition.

Product
PDIF

Privilege
Administrator, Security Administrator

Syntax

[ default ] radius accounting pdif trigger-policy { standard | counter-rollover }

default
The default option configures the “standard” policy.

standard
Applies a policy as defined by the standards.

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

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

Example
Use the following example to set the default policy to standard

default radius accounting pdif trigger-policy
radius accounting rp

Configures the RADIUS accounting R-P originated call options.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

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

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

default radius accounting rp { handoff-stop | trigger-policy }

---

no

Removes earlier configuration for the specified keyword.

---

default

Sets the default configuration for the specified keyword.

---

handoff-stop { immediate | wait-active-stop }

Default: wait-active-stop

Specifies the behavior of generating accounting STOP when handoff occurs.

*immediate: Indicates that accounting STOP should be generated immediately on handoff, i.e. not to wait active-stop from the old PCF.

*wait-active-stop: Indicates that accounting STOP is generated only when active-stop received from the old PCF when handoff occurs.

---

tod minute hour

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

minute must be an integer from 0 through 59.

hour must be an integer from 0 through 23.

---

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

Default: active-handoff: Disabled

active-start-param-change: Enabled

active-stop: Disabled

Configures the events for which a RADIUS event is generated for accounting as one of the following:
**active-handoff**: Disables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Instead, two R-P events occur (one for the Connection Setup, and the second for the Active-Start)

**active-start-param-change**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

**active-stop**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

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

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

Default: `airlink-usage`: Disabled  
`custom`:  
`active-handoff` = Disabled  
`active-start-param-change` = Disabled  
`active-stop` = Disabled  
`standard`: Enabled

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

**airlink-usage [ counter-rollover ]**: Specifies the use of Airlink-Usage RADIUS accounting policy for R-P, which generates a start on Active-Starts, and a stop on Active-Stops.

**If** the `counter-rollover` option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than \((2^{32} - 1)\) in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than \(2^32\) thus ensuring the accuracy of the count. The system, may, at its discretion, send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped. Note that a STOP/START pair is never generated unless the subscriber RP session is in the Active state, since octet/packet counts are not accumulated when in the Dormant state.

**custom**: Specifies the use of custom RADIUS accounting policy for R-P. The custom policy can consist of the following:

**active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start)

**active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

**Important**: Note that a custom trigger policy with only `active-start-param-change` enabled is identical to the `standard` trigger-policy.

**active-stop**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.
AAA Server Group Configuration Mode Commands

radius accounting rp

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

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

**trigger-stop-start**

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

**Usage**

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

**Example**

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

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

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

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

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

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

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

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

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

ip_address [ port port_number ]
Specifies the IP address of the accounting server. ip_address must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6. A maximum of 1600 RADIUS servers per context/system and 128 servers per server group can be configured. This limit includes accounting and authentication servers.
port port_number specifies the port number to use for communications. port_number must be an integer from 0 through 65535. Default is 1813.

Important: Same RADIUS server IP address and port can be configured in multiple RADIUS server group within a context.

[ encrypted ] key value
Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted. The key value must be an alpha and/or numeric string of 1 through 15 characters, or when encrypted an alpha and/or numeric string of 1 through 30 characters. The encrypted keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.
**acct-on { enable | disable }**

Default: disable
Enables and disables sending of the Accounting-On message when a new RADIUS server is added to the configuration.

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

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

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

**max messages**

Default: 0
Specifies the maximum number of outstanding messages that may be allowed to the server.
`messages` must be an integer from 1 through 256.

**oldports**

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

**priority priority**

Default: 1000
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to.
`priority` must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the `noconfirm` option, you are not asked for confirmation and multiple servers could be assigned the same priority.

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

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

**admin-status { enable | disable }**

Configures the admin-status for the RADIUS accounting server.
`enable`: Enables the RADIUS accounting server.
`disable`: Disables the RADIUS accounting server.
-noconfirm

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

Usage

Use this command to configure the RADIUS accounting servers with which the system must communicate for accounting.

Up to 1600 RADIUS servers per context/system and 128 servers per server group can be configured. The servers can be configured as Accounting, Authentication, Charging servers, or any combination thereof.

Example

The following command sets the accounting server with mediation device transaction for AAA server 1.2.3.4:

```
radius mediation-device accounting server 1.2.3.4 key sharedKey port 1024
max 127
```
radius algorithm

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

Product
All

Privilege
Security Administrator, Administrator

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

default radius algorithm

default
Configures the default setting.
Default: first-server

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

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

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

Example
radius algorithm first-server
radius algorithm round-robin
radius allow

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

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

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

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

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

Example

radius allow authentication-down
no radius allow authentication-down
radius allow accounting-down
no radius allow accounting-down
radius attribute

Configures the system’s RADIUS identification parameters.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius attribute { nas-identifier id | nas-ip-address address primary_address [ backup secondary_address ] [ nexthop-forwarding-address nexthop_address ] [ vlan vlan_id ] [ mpls-label input input output output [ integer_value ] ] }

no radius attribute { nas-identifier | nas-ip-address }

default radius attribute nas-identifier

no
Removes configuration for the specified keyword.

default
Configures the default setting.

nas-identifier id
Specifies the attribute name by which the system will be identified in Access-Request messages. id must be a case-sensitive alpha and/or numeric string of 1 through 32 characters in length.

nas-ip-address address primary_address
Specifies the AAA interface IP address(es) used to identify the system. Up to two addresses can be configured.
primary_address: The IP address of the primary interface to use in the current context. This must be specified using the standard IPv4 dotted decimal notation.

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

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

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

### mpls-label input in_label_value| output out_label_value1 [ out_label_value2 ]

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

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

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

### vlan vlan_id

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

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

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

**Usage**

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

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

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

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

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

Example

```
radius attribute nas-ip-address 1.2.3.4
no radius attribute nas-identifier sampleID
```
radius authenticate

This command configures RADIUS authentication related parameters.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius authenticate { apn-to-be-included { gi | gn } | null-username }
default radius authenticate { apn-to-be-included | null-username }
no radius authenticate null-username

default
Configures the default setting.

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

apn-to-be-included
Specifies the APN name to be included for RADIUS authentication:
gi: Specifies the usage of Gi APN name in RADIUS authentication request. Gi APN represents the APN received in the Create PDP Context request message from SGSN.
gn: Specifies the usage of Gn APN name in RADIUS authentication request. Gn APN represents the APN selected by the GGSN.

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

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

Example
To disable sending Access-Request messages for user names (NAI) that are blank, enter the following command:

```
no radius authenticate null-username
```

To re-enable sending Access-Request messages for user names (NAI) that are blank, enter the following command:

```
radius authenticate null-username
```
AAA Server Group Configuration Mode Commands

radius authenticate
radius authenticator-validation

This command enables (allows) and disables (prevents) the MD5 authentication of RADIUS user. MD5 authentication is enabled by default.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] radius authenticator-validation
```

- **no**
  Disables MD5 authentication validation for an Access-Request message to the AAA server.

**Usage**

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

**Example**

To disable MD5 authentication validation for Access-Request messages for usernames (NAI), enter the following command:

```
no radius authenticator-validation
```

To enable MD5 authentication validation for Access-Request messages for user names (NAI), enter the following command:

```
radius authenticator-validation
```
radius charging

This command configures basic RADIUS options for Active Charging Service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | default ] radius charging { deadtime dead_minutes | detect-dead-server { consecutive-failures count | response-timeout seconds } | max-outstanding messages | max-retries tries | max-transmissions transmissions | timeout idle_seconds }
```

- **no**
  Removes configuration for the specified keyword.

- **default**
  Configures the default setting for the specified keyword.

- **deadtime dead_minutes**
  Specifies the number of minutes to wait before attempting to communicate with a server that has been marked as unreachable.
  `dead_minutes` must be an integer from 0 through 65535.
  Default: 10

- **detect-dead-server { consecutive-failures count | response-timeout seconds }**
  `consecutive-failures count`: Specifies the number of consecutive failures, for each AAA Manager, before a server is marked as unreachable.
  `count` must be an integer from 1 through 1000.
  Default: 4
  `response-timeout seconds`: Specifies the number of seconds for each AAA Manager to wait for a response to any message before a server is detected as failed, or in a down state.
  `seconds` must be an integer from 1 through 65535.

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

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

**max-transmissions transmissions**

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

`transmissions` must be an integer from 1 through 65535.

Default: Disabled

**timeout idle_seconds**

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages.

`idle_seconds` must be an integer from 1 through 65535.

Default: 3

**Usage**

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

**Example**

```
radius charging detect-dead-server consecutive-failures 6
radius charging timeout 300
```
radius charging accounting algorithm

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

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

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

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

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

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

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

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

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

Configures RADIUS charging accounting servers in the current context for Active Charging Service Prepaid Accounting.

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

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

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

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

[ encrypted ] key value
Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted. The key value must be an alpha and/or numeric string of 1 through 15 characters, or an alpha and/or numeric string of 1 through 30 characters when encrypted.
The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

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

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

port port_number
Default: 1813
Specifies the port number to use for communication.
**radius charging accounting server**

`port_number` must be an integer from 0 through 65535.

**priority priority**

Default: 1000

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

**admin-status { enable | disable }**

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

**-noconfirm**

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

**Usage**

This command is used to configure the RADIUS charging accounting server(s) with which the system is to communicate for Active Charging Service Prepaid Accounting requests.

**Example**

Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

```
radius charging accounting server 1.2.3.4 key sharedKey port 1024 max 127
radius charging accounting server 1.2.5.6 encrypted key scrambledKey oldports priority 10 ]
no radius charging accounting server 1.2.5.6
```
radius charging algorithm

Specifies the RADIUS authentication server selection algorithm for Active Charging Service for the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

default radius charging algorithm
```

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

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

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

Usage

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

Example

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

Configures the RADIUS charging server(s) in the current context for Active Charging Service Prepaid Authentication.

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

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

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

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

- **[ encrypted ] key value**
  Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted. The `key value` must be an alpha and/or numeric string of 1 through 15 alpha characters, or an alpha and/or numeric string of 1 through 30 characters when encrypted. The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `key` keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

- **max messages**
  Default: 256
  Specifies the maximum number of outstanding messages that may be allowed to the server. `messages` must be an integer from 0 through 4000.

- **oldports**
  Sets the UDP communication port to the old default for RADIUS communications to 1645.

- **port port_number**
  Default: 1812
  Specifies the port number to use for communications. `port_number` must be an integer from 1 through 65535.
radius charging server

priority priority
Default: 1000
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to. 

priority must be an integer from 1 through 1000, where 1 is the highest priority.

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

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

Usage
This command is used to configure the RADIUS charging server(s) with which the system is to communicate for Active Charging Service Prepaid Authentication requests.

Example
Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

radius charging server 1.2.3.4 key sharedKey port 1024 max 127
radius charging server 1.2.5.6 encrypted key scrambledKey oldports priority 10 ]
no radius server 1.2.5.6
radius ip vrf

This command associates the specific AAA group with a Virtual Routing and Forwarding (VRF) Context instance for GRE tunnel interface configuration. By default the VRF is NULL, which means that AAA group is associated with global routing table.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius ip vrf vrf_name

no radius ip vrf

---

no
Removes/disassociates configured IP Virtual Routing and Forwarding (VRF) context instance.

---

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

Usage
Use this command to associate/disassociate a pre-configured VRF context for a GRE tunnel interface. By default the VRF is NULL, which means that AAA group is associated with global routing table.

Example
The following command associates VRF context instance GRE_vrf1 with this AAA group:

radius ip vrf GRE_vrf1
radius keepalive

This command configures the RADIUS keepalive authentication parameters.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ default ] radius keepalive [ calling-station-id id | consecutive-response number | encrypted | interval seconds | password | retries number | timeout seconds | username name | valid-response access-accept | access-reject ]
```

default
Configures the default setting for the specified keyword.

calling-station-id id
Specifies the Calling-Station-Id to be used for the keepalive authentication.
id must be an alpha and/or numeric string of 1 through 15 characters in length.
Default value is 000000000000000.

consecutive-response number
Specifies the number of consecutive authentication responses after which the server is marked as reachable.
number must be an integer from 1 through 5.
Default: 1

encrypted password
Specifies encrypting the password.
password must be an alpha and/or numeric string of 1 through 64 characters in length.
Default password: Test-Password

interval seconds
Specifies the time interval, in seconds, between two keepalive access requests.
Default: 30 seconds

password
Specifies the password to be used for authentication.
password must be an alpha and/or numeric string of 1 through 64 characters in length.
Default password: Test-Password

retries number
Specifies the number of times the keepalive access request to be sent before marking the server as unreachable.
number must be an integer from 3 through 10.
Default: 3
timeout seconds
Specifies the time interval between keepalive access request retries.
seconds must be an integer from 1 through 30.
Default: 3 seconds

username name
Specifies the user name to be used for authentication. name must be an alpha and/or numeric string of 1 through 127 characters in length.
Default: Test-Username

valid-response access-accept [ access-reject ]
Specifies the valid response for the authentication request.
If access-reject is configured, then both access-accept and access-reject are considered as success for the keepalive authentication request.
If access-reject is not configured, then only access-accept is considered as success for the keepalive access request.
Default: keepalive valid-response access-accept

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

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

radius keepalive username Test-Username2

The following command configures the number of RADIUS keepalive retries to 4:

radius keepalive retries 4
radius mediation-device

See the radius accounting server command.
radius probe-interval

This command configures the time interval between two RADIUS authentication probes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
radius probe-interval seconds
```

```
default radius probe-interval
```

```
default
Configures the default setting.
```

```
seconds
Default: 60
Specifies the number of seconds to wait before sending another probe authentication request to a RADIUS server.
seconds must be an integer from 1 through 65535.
```

**Usage**

Use this command for Interchassis Session Recovery (ICSR) support to set the duration between two authentication probes to the RADIUS server.

**Example**

The following command sets the RADIUS authentication probe interval to 30 seconds.

```
radius probe-interval 30
```
radius probe-max-retries

This command configures the number of retries for RADIUS authentication probe response.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius probe-max-retries retries

default radius probe-max-retries

retries
Default: 5
Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed.
retries must be an integer from 0 through 65535.

Usage
Use this command for Home Agent Geographical Redundancy (HAGR) support to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

Example
The following command configures the maximum number of retries to 6 seconds.

radius probe-max-retries 6
radius probe-timeout

This command configures the timeout duration for HAGR to wait for a response for RADIUS authentication probes.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius probe-timeout idle_seconds

default radius probe-timeout

default
Configures the default setting.

idle_seconds
Default: 3
Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the authentication probe.
idle_seconds must be an integer from 0 through 65535.

Usage
Use this command for Home Agent Geographical Redundancy (HAGR) support to set the time duration to wait for response before re-sending the RADIUS authentication probe to the RADIUS server.

Example
The following command sets the authentication probe timeout to 120 seconds:

radius probe-timeout 120
radius server

This command configures RADIUS authentication server(s) in the current context for authentication.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius server ip_address [ encrypted ] key value [ max messages ] [ oldports ] [ port port_number ] [ priority priority ] [ probe | no-probe ] [ probe-username username ] [ probe-password [ encrypted ] password password ] [ type { mediation-device | standard } ] [ admin-status { enable | disable } ] [ -noconfirm ]

no radius server ip_address [ oldports | port port_number ]

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

[ encrypted ] key value

Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted. The key value must be an alpha and/or numeric string of 1 through 15 characters, or an alpha and/or numeric string of 1 through 30 characters when encrypted. The encrypted keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

max messages

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

priority priority
Default: 1000
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to.
priority must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the -noconfirm option, you are not asked for confirmation and multiple servers could be assigned the same priority.

probe
Enable probe messages to be sent to the specified RADIUS server.

no-probe
Disable probe messages from being sent to the specified RADIUS server. This is the default behavior.

probe-username username
The username sent to the RADIUS server to authenticate probe messages. username must be an alpha and/or numeric string of 1 through 127 characters in length.

probe-password [ encrypted ] password password
The password sent to the RADIUS server to authenticate probe messages.
encrypted: This keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
password password: Specifies the probe-user password for authentication. password must be an alpha and/or numeric string of 1 through 63 characters in length.

type { mediation-device | standard }
Specifies the type of transactions the RADIUS server accepts.
mediation-device: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local sales representative for licensing information.
standard - Specifies standard AAA transactions. (Default)

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

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

Usage
This command is used to configure the RADIUS authentication server(s) with which the system is to communicate for authentication. Up to 1600 RADIUS servers per context/system and 128 servers per Server group can be configured. The servers can be configured as accounting, authentication, charging servers, or any combination thereof.

Example

```
radius server 1.2.3.4 key sharedKey port 1024 max 127
radius server 1.2.5.6 encrypted key scrambledKey oldports priority 10
no radius server 1.2.5.6
```
Chapter 3
AAL2 Node Configuration Mode Commands

The AAL2 Node Configuration Mode is used to configure the ATM Adaptation Layer 2 nodes to manage the Access Link Control Application Part (ALCAP) on HNB-GW for IuCS-over-ATM support towards CS core network.

Important: The AAL2 Node configured here will be used to bind with ATM port in PVC configuration sub-mode of ATM configuration mode for IuCS-over-ATM functionality.
**aal2-path-id**

This command sets the AAL2 path identifier with AAL2 node and also used to block a particular AAL2 path.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] aal2-path-id aal2_path_id [block]
```

*no*

Removes the configured AAL2 path identifier from this AAL2 node configuration.

```
aal2_path_id
```

Specifies the AAL2 path identifier configured with adjacent AAL2 node(s). The AAL2 path id must be unique within an AAL2 node configuration. This value is used to identify a particular path towards an adjacent AAL2 node and is sent in ALCAP protocol messages to peer where path identification is required. The `aal2_path_id` must be an integer between 1 through 16.

**Important:** This AAL2 path id `aal2_path_id` will be used to bind with ATM port in PVC configuration mode of ATM configuration mode.

**block**

This keyword blocks the AAL2 path configured with specific path identifier. When this keyword is executed ALCAP-BLO-REQUEST shall be sent to the adjacent AAL2 node. To unblock an AAL2 path, the no keyword will be used for a locally blocked path by sending ALCAP-UNBLOCK-REQUEST to the adjacent AAL2 node.

**Usage**

Use this command to configure an AAL2 path between a pair of adjacent nodes, which is identified by a unique number called AAL2 path identifier. An AAL2 path provides 248 AAL2 channels wherein each AAL2 channel is used for one circuit switched call. The AAL2 channel range defined is 8 to 255. This command can be used for blocking or unblocking an AAL2 path towards an adjacent AAL2 node.

**Important:** The AAL2 path id configured here will be used to bind with ATM port in PVC configuration sub-mode of ATM configuration mode for IuCS-over-ATM functionality.

**Example**

Following command sets the AAL2 path identifier `2` in an AAL2 node configuration.

```
aal2-path-id 2
```
Following command unblocks the AAL2 path identifier 6 which was earlier blocked in an AAL2 node configuration.

```bash
no a2-path-id 6 block
```
end

Exits the current mode and returns to the Exec Mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`end`

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the previous mode.
point-code

This command configure the point code of adjacent AAL2 node in SS7 format address. This point code shall be filled in the destination point-code (dpc) field of MTP3 routing label. This is required if signaling transport network is based on MTP3-broadband (MTP3B).

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[no] point-code point_code
```

**no**

Removes the configured point code from this AAL2 node configuration.

**point_code**

Defines the point code to assign to adjacent AAL2 node in SS7 format.

- value entered must adhere to the point code variant selected when the AAL2 node was defined:
  - ITU Range 0.0.1 to 7.255.7
  - ANSI Range 0.0.1 to 255.255.255
  - TTC Range 0.0.1 to 15.31.255
  - a string of 1 to 11 combined digits ad period.

**Usage**

Use this command to configure configure the point code of adjacent AAL2 node in SS7 format address. This point code shall be filled in the destination point-code (dpc) field of MTP3 routing label. This is required if signaling transport network is based on MTP3-broadband (MTP3B).

A maximum of TBD point codes for adjacent AAL2 nodes can be configured in one ALCAP service.

**Example**

The following command configures the point code 4.121.5 for adjacent AAL2 node.

```
point-code 4.121.5
```

The following command removes the point code 4.121.15 from AAL2 node configuration.

```
no point-code 4.121.15
```
Chapter 4
Accounting Policy Configuration Mode Commands

The Accounting Policy Configuration Mode is used to define the accounting method, mode, and event trigger responses for the accounting policy supporting the Rf (off-line charging) interface.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          policy accounting name
            Accounting Policy Configuration Mode
```
accounting-event-trigger

Configures the response to specific event triggers for this policy. Multiple event instances can be configured.

**Product**
HSGW, P-GW, S-GW

**Privilege**
Administrator

**Syntax**

```plaintext
accounting-event-trigger { flow-information-change | interim-timeout | location-change } action { interim | stop-start }

[ default | no ] accounting-event-trigger { flow-information-change | interim-timeout | location-change }
```

- **default**
  Returns the command to its default setting of interim for the `action` keyword (for all events).

- **no**
  Removes the specified event trigger configuration from this policy.

- **flow-information-change**
  Specifies that the action is initiated upon indication of a change in the flow information.

- **interim-timeout**
  Specifies that the action is initiated upon expiration of the interim interval.

- **location-change**
  Specifies that the action is initiated upon indication of

- **action { interim | stop-start }**
  Default: interim
  Specifies the action initiated upon the occurrence of an event.

- **interim**
  Specifies that an interim ACR is sent.

- **stop-start**
  Specifies that a stop-start ACR is sent.

**Usage**

Use the `is` command to configure that action taken upon the occurrence on an accounting event trigger.

**Example**

The following command configures the policy to send a stop-start ACR upon indication of an interim timeout:

```plaintext
accounting-event-trigger interim-timeout
```
accounting-level

Configures the type of accounting performed by this profile.

Product
HSGW, P-GW, S-GW

Privilege
Administrator

Syntax

accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }

default accounting-level

default
Returns the command to the default setting of subscriber-based accounting.

flow
Specifies that flow-based accounting is to be used for this accounting profile. Accounting Request (ACR) Start messages include an AVP with the following EPS information:

- PDN identifier
- QCI for which accounting is done
- Charging rule name for which accounting is being done
- AF charging identifier (included if PCRF has provided a charging identifier to correlate AF generated information)
- Flow description for the flows
- User Equipment information if available (ESN/MEID)
- Address of HSGW/SGW
- Address of the PGW (if available), one or more instances

pdn
Specifies that PDN-based accounting is to be used for this accounting profile. Accounting Request (ACR) Start messages include an AVP with the following EPS information:

- Addresses allocated to the UE in this PDN
- PDN identifier
- User Equipment information if available (ESN/MEID)
- Address of HSGW/SGW
- Address of the PGW (if available), one or more instances

pdn-qci
Specifies that PDN-QCI accounting is to be used for this accounting profile. Accounting Request (ACR) Start messages include an AVP with the following EPS information:

- Addresses allocated to the UE in this PDN
• PDN identifier
• QCI for which accounting is done
• User Equipment information if available (ESN/MEID)
• Address of HSGW/SGW
• Address of the PGW (if available), one or more instances

```qci```
Specifies that QCI-based accounting is to be used for this accounting profile. Accounting Request (ACR) Start messages include an AVP with the following EPS information:

- QCI for which accounting is done
- User Equipment information if available (ESN/MEID)
- Address of HSGW/SGW
- Address of the PGW (if available), one or more instances

```sdf```
Specifies that service data flow accounting is to be used for this accounting profile. Accounting Request (ACR) Start messages include an AVP with the following EPS information:

```subscriber```
Specifies that subscriber-based accounting is to be used for this accounting profile. Accounting Request (ACR) Start messages include an AVP with the following EPS information:

- User Equipment information if available (ESN/MEID)
- Address of HSGW/SGW
- Address of the PGW (if available), one or more instances

**Usage**
Use this command to specify the type of accounting performed by this profile.

**Example**
The following command sets the accounting type for this profile to flow-based:

```
accounting-level flow
```
accounting-mode

Configures the accounting mode for this profile.

Product
HSGW, P-GW, S-GW

Privilege
Administrator

Syntax

accounting-mode normal

default accounting-mode

default
Returns the accounting mode for this profile to its default setting of “normal”.

normal
Specifies that “normal” (start/interim/stop) accounting will be performed for this profile.

Usage

Use this command to set the accounting mode for this profile.
cc profile

Configures a charging characteristics profile, within the accounting profile configuration, for CDR generation.

Product
S-GW

Privilege
Administrator

Syntax

```
cc profile index { buckets num | interval seconds | tariff time1 min hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } } }

default cc profile index

no cc profile index { buckets | interval | tariff | volume }
```

**Default**

Returns all profile features, for the specified profile index, to their default settings.

**No**

Returns the specified feature to its default setting.

**Profile index**

Specifies a billing type to be applied to this profile. `index` must be one of the following:

- 1: Hot billing
- 2: Flat billing
- 4: Prepaid billing
- 8: Normal billing

**buckets num**

Default: 4

Specifies the number of container changes in the S-GW CDR due to QoS changes or tariff times. `num` must be an integer value from 1 to 4. If an accounting policy is not configured, this value is 4.

**interval seconds**

Default: disabled

Specifies a time interval for closing the charging record if the minimum volume thresholds are satisfied. `seconds` must be an integer value from 60 to 40000000.

**tariff time1 min hrs [ time2 min hrs...time4 min hrs ]**

Specifies time-of-day values used to determine when a container is closed in the charging records. `time1 min hrs`: Specifies the first time-of-day value used to close the current container in the charging record. `min` must be an integer value from 0 to 59. `hrs` must be an integer value from 0 to 23.
Accounting Policy Configuration Mode Commands

cc profile

- time2 min hrs...time4 minutes hours: Specifies the second, third and fourth time-of-day values used to close containers in the charging record. min must be an integer value from 0 to 59, hrs must be an integer value from 0 to 23.

volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } }

Specifies octet volume thresholds for the generation of interim CDRs.
- downlink octets: Sets the threshold limit for the number of downlink octets that must be reached before the charging record is closed. octets must be an integer value from 100000 to 40000000000.
- total octets: Sets the threshold limit for the total number of octets that must be reached before the charging record is closed. octets must be an integer value from 100000 to 40000000000.
- uplink octets: Sets the threshold limit for the number of uplink octets that must be reached before the charging record is closed. octets must be an integer value from 100000 to 40000000000.

Usage
Use this command to set charging characteristics that directly affect the CDR generation on the S-GW.

Example
The following command creates a hot billing profile with a total octet volume threshold set to 500,000:

cc profile 1 volume total 500000
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
`end`

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
operator-string

Configures a text string to be included with accounting messages sent by this policy.

Product
HSGW, P-GW, S-GW

Privilege
Administrator

Syntax

operator-string string

no operator-string

no
Removes the operator string from this policy.

string
Specifies a text string that is included with accounting messages originating from this policy. string must be from 1 to 63 alpha and/or numeric characters.

Usage
Use this command to create a text string to be included with accounting messages originating from this policy.

Example
The following command creates the text string “pgw_local” to be included with accounting messages originating from this policy:

operator-string pgw_local
Chapter 5
ACL Configuration Mode Commands

The Access Control List Configuration Mode is used to create and manage IP access privileges.
deny/permit

The following commands set access permissions based on various parameters:
deny/permit (by source IP address masking)

Used to filter subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
{ deny | permit } [ log ] source_address source_wildcard
after { deny | permit } [ log ] source_address source_wildcard
before { deny | permit } [ log ] source_address source_wildcard
no { deny | permit } [ log ] source_address source_wildcard
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**deny | permit**
Specifies the rule is either block (deny) or an allow (permit) filter.
- **deny**: indicates the rule, when matched, drops the corresponding packets.
- **permit**: indicates the rule, when matched, allows the corresponding packets.

**log**
Default: packets are not logged. Indicates all packets which match the filter are to be logged.
deny/permit (by source IP address masking)

source_address
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

Usage
Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rules as it does not require a rule for each source and destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

Example
The following command defines two rules with the second logging filtered packets.
permit 1.2.3.0 0.0.0.31
deny log 1.2.4.0 0.0.0.15
The following sets the insertion point before the first rule defined above.
before permit 1.2.3.0 0.0.0.31
The following command sets the insertion point after the second rule defined above.
after deny log 1.2.4.0 0.0.0.15
The following deletes the first rule defined above.
no permit 1.2.3.0 0.0.0.31
deny/permit (any)

Used to filter subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
{ deny | permit } [ log ] any
after { deny | permit } [ log ] any
before { deny | permit } [ log ] any
no { deny | permit } [ log ] any
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**deny | permit**
Specifies the rule is either block (deny) or an allow (permit) filter.
deny: indicates the rule, when matched, drops the corresponding packets.
permit: indicates the rule, when matched, allows the corresponding packets.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

\textbf{deny/permit (any)}

\textbf{any}

Indicates all packets will match the filter regardless of source and/or destination.

\section*{Usage}

Define a catch all rule to place at the end of the list of rules.

\textbf{Important:} It is suggested that any rule which is added to be a catch all should also have the \texttt{log} option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

\section*{Example}

The following commands define two rules with the second logging filtered packets.

\begin{verbatim}
permit any
deny log any
before permit any
after deny log any
no permit any
\end{verbatim}

deny/permit (by host IP address)

Used to filter subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

{ deny | permit } [ log ] host source_host_address

after { deny | permit } [ log ] host source_host_address

before { deny | permit } [ log ] host source_host_address

no { deny | permit } [ log ] host source_host_address

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

deny: indicates the rule, when matched, drops the corresponding packets.

permit: indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
deny/permit (by host IP address)

Indicates all packets which match the filter are to be logged.

source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.

Usage
Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

Example
The following commands define two rules with the second logging filtered packets.

**permit host 1.2.3.4**
**denylog host 1.2.3.5**
The following sets the insertion point before the first rule defined above.
**before permit host 1.2.3.4**
The following command sets the insertion point after the second rule defined above.
**after denylog host 1.2.3.5**
The following deletes the first rule defined above.
**no permit host 1.2.3.4**
deny/permit (by source ICMP packets)

Used to filter subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[
\begin{align*}
\text{after} & \{ \text{deny} | \text{permit} \} [ \log ] \text{ icmp } \{ \text{source_address} \text{ source wildcard} | \text{any} | \text{host} \text{source_host_address} \} \{ \text{dest_address} \text{ dest wildcard} | \text{any} | \text{host} \text{dest_host_address} \} [ \text{icmp_type} [ \text{icmp_code} ] ] \\
\text{before} & \{ \text{deny} | \text{permit} \} [ \log ] \text{ icmp } \{ \text{source_address} \text{ source wildcard} | \text{any} | \text{host} \text{source_host_address} \} \{ \text{dest_address} \text{ dest wildcard} | \text{any} | \text{host} \text{dest_host_address} \} [ \text{icmp_type} [ \text{icmp_code} ] ] \\
\text{no} & \{ \text{deny} | \text{permit} \} [ \log ] \text{ icmp } \{ \text{source_address} \text{ source wildcard} | \text{any} | \text{host} \text{source_host_address} \} \{ \text{dest_address} \text{ dest wildcard} | \text{any} | \text{host} \text{dest_host_address} \} [ \text{icmp_type} [ \text{icmp_code} ] ]
\end{align*}
\]

\textbf{after}
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

\textbf{Important:} If the options specified do not exactly match an existing rule, the insertion point does not change.

\textbf{before}
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

\textbf{Important:} If the options specified do not exactly match an existing rule, the insertion point does not change.

\textbf{no}
Removes the rule which exactly matches the options specified.
deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

*deny*: indicates the rule, when matched, drops the corresponding packets.

*permit*: indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

device

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- **Zero-bits** in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.

- **One-bits** in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in dotted decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in dotted decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `destWildcard` parameter.
This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Example**
The following commands define two rules with the second logging filtered packets.

```
permit icmp host 1.2.3.4 any 168
deny log icmp 1.2.3.0 0.0.0.31 host 1.2.4.16 168 11
```

The following sets the insertion point before the first rule defined above.

```
before permit icmp host 1.2.3.4 any 168
```

The following command sets the insertion point after the second rule defined above.

```
after deny log icmp 1.2.3.0 0.0.0.31 host 1.2.4.16 168 11
```

The following deletes the first rule defined above.

```
no permit icmp host 1.2.3.4 any 168
```
deny/permit (by IP packets)

Used to filter subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
{ deny | permit } [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ fragment ] [ protocol num ]

after { deny | permit } [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ fragment ] [ protocol num ]

before { deny | permit } [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ fragment ] [ protocol num ]

no { deny | permit } [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ fragment ] [ protocol num ]
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.
deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

deny: indicates the rule, when matched, drops the corresponding packets.
permit: indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source wildcard parameter.

source wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in dotted decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in dotted decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest wildcard parameter.
ACL Configuration Mode Commands

**deny/permit (by IP packets)**

- **dest_wildcard**
  This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

- **fragment**
  Indicates packet filtering is to be applied to IP packet fragments only.

- **protocol num**
  Indicates that the packet filtering is to be applied to a specific protocol number. *num* can be any integer ranging from 0 to 255.

**Important:** This keyword is not applicable to a SPIO interface. Instead, you must specify the type of protocol packets for which you want to deny/permit processing on a SPIO. For example, `deny icmp`, `deny tcp`, or `deny udp`.

**Usage**
Block IP packets when the source and destination are of interest.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Example**
The following commands define two rules with the second logging filtered packets.

```plaintext
permit ip host 1.2.3.4 any fragment
deny log ip 1.2.3.0 0.0.0.31 host 1.2.4.16
```

The following sets the insertion point before the first rule defined above.

```plaintext
before permit ip host 1.2.3.4 any fragment
```

The following command sets the insertion point after the second rule defined above.

```plaintext
after deny log ip 1.2.3.0 0.0.0.31 host 1.2.4.16
```

The following deletes the first rule defined above.

```plaintext
no permit ip host 1.2.3.4 any fragment
```
deny/permit (by TCP/UDP packets)

Used to filter subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
{ deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any |
host source_host_address } [ eq source_port | gt source_port | lt source_port |
neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address |
eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ]
}

after { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard |
any | host source_host_address } [ eq source_port | gt source_port | lt source_port |
neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address |
eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ]
}

before { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard |
any | host source_host_address } [ eq source_port | gt source_port | lt source_port |
neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address |
eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ]
}

no { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard |
any | host source_host_address } [ eq source_port | gt source_port | lt source_port |
neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address |
eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ]
}
```

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**Important:** Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

---

**Important:** Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

deny | permit
Specifies the rule is either block (deny) or an allow (permit) filter.
deny: indicates the rule, when matched, drops the corresponding packets.
permit: indicates the rule, when matched, allows the corresponding packets.

log
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

tcp | udp
Specifies the filter is to be applied to IP based transmission control protocol or the user datagram protocol.
tcp: filter applies to TPC packets.
udp: filter applies to UDP packets.

**source_address**
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the **source_wildcard** parameter.

**source_wildcard**
This option is used in conjunction with the **source_address** option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.
**source_host_address**
The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in dotted decimal notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **destWildcard** parameter.

**destWildcard**
This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  • Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
  • One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**eq dest_port**
Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to any integer value from 0 to 65535.
deny/permit (by TCP/UDP packets)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>gt dest_port</strong></td>
<td>Specifies that all destination TCP port numbers greater than the one specified are to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td><strong>lt dest_port</strong></td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td><strong>neq dest_port</strong></td>
<td>Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td><strong>range start_port end_port</strong></td>
<td>Specifies a range of ports to be matched. start_port must be an integer from 0 to 65535, and must be less than the end_port value. end_port must be an integer from 0 to 65535, and must be greater than the start_port value.</td>
</tr>
</tbody>
</table>

**Important:** This option is supported in PDIF Release 8.3.

**Usage**
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Example**
The following commands define four rules with the second and fourth rules logging filtered packets.

```plaintext
permit tcp host 1.2.3.4 any
deny log udp 1.2.3.0 0.0.0.31 host 1.2.4.16
permit tcp host 1.2.3.64 gt 1023 any
deny log udp 1.2.3.0 0.0.0.31 1.2.4.127 0.0.0.127
```
The following sets the insertion point before the first rule defined above.

```plaintext
before permit tcp host 1.2.3.4 any
```
The following command sets the insertion point after the second rule defined above.

```plaintext
after deny log udp 1.2.3.0 0.0.0.31 host 1.2.4.16
```
The following deletes the third rule defined above.

```plaintext
no permit tcp host 1.2.3.64 gt 1023 any
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.

Example
end
exit

Exits the ACL configuration mode and returns to the context configuration mode.

Privilege
Security Administrator, Administrator

Product
All

Syntax
```
exit
```

Usage
Return to the context configuration mode.

Example
```
exit
```
readdress server

Alter the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

readdress server

redirect_address [ portport_no ] ( tcp | udp ) { { source_address
source_wildcard | any | hostsource_host_address } [ eqsource_port |
gtsource_port | ltsource_port | neqsource_port ] } { { dest_address
dest_wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | neqdest_port ] }

before

after

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

after

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the
exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified
such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

Before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the
exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified
such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

`no`

Removes the rule which exactly matches the options specified.

---

`redirect_address`

The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must be an IPv4 address specified in dotted decimal notation.

---

`port port_no`

The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.

---

`tcp | udp`

Specifies the redirect is to be applied to the IP based transmission control protocol or the user datagram protocol.

- `tcp`: redirect applies to TCP packets.
- `udp`: redirect applies to UDP packets.

---

`source_address`

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

---

`source_wildcard`

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

---

`any`

Specifies that the rule applies to all packets.

---

`host`

Specifies that the rule applies to a specific host as determined by its IP address.
source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in dotted decimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest wildcard parameter.

dest wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
● Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
● One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to any integer value from 0 to 65535.
**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

**neq dest_port**

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

---

**Usage**

Use this command to define a rule that redirects packets to a different destination address. The TCP and UDP packet headers are modified with the new destination address and destination port.

---

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important:** Prior to Release 8.3, for packets received from the packet data network destined for a subscriber's UE, the system applied logic to reset the source address of a packet to the original destination address of the input packet before applying the outbound access control list (ACL). In Release 8.3 and higher, the system reverses the order and applies the outbound ACL before resetting the source address. This change impacts all current readdress server rules in inbound IPv4 ACLs.

**Important:** After upgrading to Release 8.3, for every readdress server rule in an inbound IPv4 ACL, customers must now add a permit rule to an outbound ACL that explicitly permits packets from the readdress rule's redirect address and port number. If customers omit this permit rule, the system will reject all packets destined for the subscriber's UE from the readdress rule's redirect address and port number.

---

**Example**

The following command defines a rule that redirects packets to the server at 192.168.10.4, UDP packets coming from any host with a destination of any host are matched.

```
readdress server 192.168.10.4 udp any any
```

The following sets the insertion point before the rule defined above.

```
before readdress server 192.168.10.4 udp any any
```

The following sets the insertion point after the first rule defined above.

```
after readdress server 192.168.10.4 udp any any
```

The following deletes the rule defined above.

```
o readdress server 192.168.10.4 udp any any
```
redirect context

The following commands redirect subscriber sessions to a different context based on various parameters:
redirect context (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect context context_id [ log ] source_address source_wildcard
after redirect context context_id [ log ] source_address source_wildcard
before redirect context context_id [ log ] source_address source_wildcard
noredirect context context_id [ log ] source_address source_wildcard
```

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**

Removes the rule which exactly matches the options specified.

```
context context_id
```

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.
**source_address**

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule that redirects packets to the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31.

```
redirect context 23 192.168.22.0 0.0.0.31
```

The following sets the insertion point before the rule defined above.

```
before redirect context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the first rule defined above.

```
after redirect context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above.

```
no redirect context 23 198.162.22.0 0.0.0.31
```
redirect context (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

redirect context context_id [ log ] any  

after redirect context context_id [ log ] any  

before redirect context context_id [ log ] any  

no redirect context context_id [ log ] any

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**context context_id**
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.
any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: It is suggested that any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

Important: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the context with the context ID of 23 and any source IP.

```redirect context 23 any```

The following sets the insertion point before the rule defined above.

```before redirect context 23 any```

The following command sets the insertion point after the first rule defined above.

```after redirect context 23 any```

The following deletes the first rule defined above.

```no redirect context 23 any```
redirect context (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

redirect context context_id [ log ] host source_ip_address
after redirect context context_id [ log ] host source_ip_address
before redirect context context_id [ log ] host source_ip_address
noredirect context context_id [ log ] host source_ip_address

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

log
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.
host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.

Usage
Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

⚠️ Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

⚠️ Important: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the context with the context ID of 23 and a host IP address of 192.168.200.11.

```
redirect context 23 host 192.168.200.11
```

The following sets the insertion point before the rule defined above.
```
before redirect context 23 host 192.168.200.11
```

The following command sets the insertion point after first the rule defined above.
```
after redirect context 23 host 192.168.200.11
```

The following deletes the first rule defined above.
```
no redirect context 23 host 192.168.200.11
```
redirect context (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

after redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

before redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

no redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule applies to all packets.

**host**

Specifies that the rule applies to a specific host as determined by its IP address.

**sourceHostAddress**

The IP address of the source host to filter against expressed in dotted decimal notation.

**destHostAddress**

The IP address of the destination host to filter against expressed in dotted decimal notation.

**destAddress**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `destWildcard` parameter.
**dest_wildcard**

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25.

```
redirect context 23 icmp host 192.168.100.25
```

The following sets the insertion point before the rule defined above.

```
before redirect context 23 icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule defined above.

```
after redirect context 23 icmp host 192.168.100.25
```

The following deletes the first rule defined above.

```
o redirect context 23 icmp host 192.168.100.25
```
redirect context (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect context context_id [ log ] ip { source_address source_wildcard | any | host [source_host_address] { dest_address dest_wildcard | any | host [dest_host_address] } [ fragment] [ protocol num ]
```

```
after redirect context context_id [ log ] ip { source_address source_wildcard | any | host [source_host_address] } { dest_address dest_wildcard | any | host [dest_host_address] } [ fragment] [ protocol num ]
```

```
befor e redirect context context_id [ log ] ip { source_address source_wildcard | any | host [source_host_address] } { dest_address dest_wildcard | any | host [dest_host_address] } [ fragment] [ protocol num ]
```

```
no redirect context context_id [ log ] ip { source_address source_wildcard | any | host [source_host_address] } { dest_address dest_wildcard | any | host [dest_host_address] } [ fragment] [ protocol num ]
```

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**no**

Removes the rule which exactly matches the options specified.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule applies to all packets.

**host**

Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in dotted decimal notation.

**dest_address**

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
**destWildcard**
This option is used in conjunction with the **destAddress** option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the **destAddress** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **destAddress** parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**fragment**
Indicates packet redirection is to be applied to IP packet fragments only.

**protocol num**
Indicates that the packet filtering is to be applied to a specific protocol number.
**num** can be any integer ranging from 0 to 255.

**Usage**
Block IP packets when the source and destination are of interest.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important**: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule that redirects packets to the context with the context ID of 23, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched.

```
redirect context 23 ip host 198.162.100.25 any fragment
```
The following sets the insertion point before the rule defined above.

```
before redirect context 23 ip host 198.162.100.25 any fragment
```
The following command sets the insertion point after the first rule defined above.

```
after redirect context 23 ip host 198.162.100.25 any fragment
```
The following deletes the first rule defined above.

```
no redirect context 23 ip host 198.162.100.25 any fragment
```
redirect context (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | hostsource_host_address } [ eqsource_port |
gtsource_port | ltsource_port | neqsource_port ] } { { dest_address
dest_wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | negdst_port ] }
```

```
after redirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | hostsource_host_address } [ eqsource_port |
gtsource_port | ltsource_port | neqsource_port ] } { { dest_address
dest_wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | negdst_port ] }
```

```
before redirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | hostsource_host_address } [ eqsource_port |
gtsource_port | ltsource_port | neqsource_port ] } { { dest_address
dest_wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | negdst_port ] }
```

```
noredirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | hostsource_host_address } [ eqsource_port |
gtsource_port | ltsource_port | neqsource_port ] } { { dest_address
dest_wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | negdst_port ] }
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**no**
Removes the rule which exactly matches the options specified.

---

`context context_id`
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

---

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

---

`tcp | udp`
Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
- `tcp`: redirect applies to TCP packets.
- `udp`: redirect applies to UDP packets.

---

**source_address**
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

---

**sourceWildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

---

**any**
Specifies that the rule applies to all packets.

---

**host**
Specifies that the rule applies to a specific host as determined by its IP address.
source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in dotted decimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the destWildcard parameter.

destWildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
• Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
• One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to any integer value from 0 to 65535.
gt dest_port

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. 
dest_port must be configured to any integer value from 0 to 65535.

lt dest_port

Specifies that all destination TCP port numbers less than the one specified are to be filtered. 
dest_port must be configured to any integer value from 0 to 65535.

neq dest_port

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. 
dest_port must be configured to any integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23, and UDP packets coming from any host are matched.

```
redirect context 23 udp any
```

The following sets the insertion point before the rule defined above.

```
before redirect context 23 udp any
```

The following command sets the insertion point after the first rule defined above.

```
after redirect context 23 udp any
```

The following deletes the rule defined above.

```
no redirect context 23 udp any
```
redirect css delivery-sequence

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.
redirect css service

The following commands redirect subscriber sessions to Content Service Steering (CSS) services based on various parameters:
redirect css service (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name [log] any
before redirect css service svc_name [log] any
after redirect css service svc_name [log] any
no redirect css service svc_name [log] any
```

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important**: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definitions which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important**: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging all` command to display the names of all configured charging services.
`svc_name` must be a string from 1 through 15 characters in length.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule definition that redirects packets to the charging service with the name `chgsvc1` and any source IP.

```
redirect css service chgsvc1 any
```

The following sets the insertion point before the rule definition above.

```
before redirect service chgsvc1 any
```

The following command sets the insertion point after the first rule definitions above.

```
after redirect service chgsvc1 any
```

The following deletes the first rule definition above.

```
no redirect service chgsvc1 any
```
redirect css service (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[ log] host source_host_address
before redirect css service svc_name[ log] host source_host_address
after redirect css service svc_name[ log] host source_host_address
no redirect css service svc_name[ log] host source_host_address
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

**log**
Default: packets are not logged.
redirect css service (by host IP address)

Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name chgsvc1 and a host IP address of 192.168.200.11.

```
redirect css service chgsvc1 host 192.168.200.11
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvc1 host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above.

```
after redirect css service chgsvc1 host 192.168.200.11
```

The following deletes the first rule definition above.

```
no redirect css service chgsvc1 host 192.168.200.11
```
redirect css service (by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service svc_name[ log] icmp { any | host source_host_address | source_address source wildcard } { any | host dest_host_address | dest_address dest wildcard } [ icmp_type[ icmp_code ]
```

```
before redirect css service svc_name[ log] icmp { any | host source_host_address | source_address source wildcard } { any | host dest_host_address | dest_address dest wildcard } [ icmp_type[ icmp_code ]
```

```
after redirect css service svc_name[ log] icmp { any | host source_host_address | source_address source wildcard } { any | host dest_host_address | dest_address dest wildcard } [ icmp_type[ icmp_code ]
```

```
no redirect css service svc_name[ log] icmp { any | host source_host_address | source_address source wildcard } { any | host dest_host_address | dest_address dest wildcard } [ icmp_type[ icmp_code ]
```

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

---

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

---

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

**no**

Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string from 1 through 15 characters in length.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule definition applies to all packets.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in dotted decimal notation.

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `destWildcard` parameter.
**dest wildcard**

This option is used in conjunction with the **dest address** option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest address** parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the **dest address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named **chgsvc1**, and ICMP packets coming from the host with the IP address **198.162.100.25**.

```bash
redirect css service chgsvc1 icmp host 192.168.200.11
```

The following sets the insertion point before the rule definition above.

```bash
before redirect css service chgsvc1 icmp host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above.

```bash
after redirect css service chgsvc1 icmp host 192.168.200.11
```

The following deletes the first rule definition above.

```bash
no redirect css service chgsvc1 icmp host 192.168.200.11
```
redirect css service (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service svc_name[ log]ip {any|host source_host_address|source_address sourceWildcard}{any|host dest_host_address|dest_address destWildcard}{fragment]
before redirect css service svc_name[ log]ip {any|host source_host_address|source_address sourceWildcard}{any|host dest_host_address|dest_address destWildcard}{fragment]
after redirect css service svc_name[ log]ip {any|host source_host_address|source_address sourceWildcard}{any|host dest_host_address|dest_address destWildcard}{fragment]
no redirect css service svc_name[ log]ip {any|host source_host_address|source_address sourceWildcard}{any|host dest_host_address|dest_address destWildcard}{fragment]
```

```
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.
```

```
before
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.
```

```
no
Removes the rule definition that exactly matches the options specified.
```
**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

*svc_name* must be a string from 1 through 15 characters in length.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule definition applies to all packets.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in dotted decimal notation.

**dest_address**

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
dest_wildcard

This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**

Block IP packets when the source and destination are of interest.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named chgsvc1, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched.

```
redirect css service chgsvc1 ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvc1 ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the first rule definition above.

```
after redirect css service chgsvc1 ip host 198.162.100.25 any fragment
```

The following deletes the first rule definition above.

```
no redirect css service chgsvc1 ip host 198.162.100.25 any fragment
```
redirect css service (by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[log] source_address source_wildcard
before redirect css service svc_name[log] source_address source_wildcard
after redirect css service svc_name[log] source_address source_wildcard
no redirect css service svc_name[log] source_address source_wildcard
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
`svc_name` must be a string from 1 through 15 characters in length.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.
source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important: A maximum of 16 rule definitions can be configured per ACL.

Example

The following command defines a rule definition to redirect packets to a charging service named chgsvc1.

redact css service chgsvc1 1.2.3.0 0.0.0.31
redirect css service (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service \(svc_{name}[log]~\{tcp|udp\}\{eq|neq|lt|gt|range\} \{source_{address}|source_{wildcard}\}\{any|host source_{host}_{address}\}\{source_{port}|eq source_{port}|gt source_{port}|lt source_{port}|neq source_{port}|range start source_{port} end source_{port}\}\{dest_{address}|dest_{wildcard}\}\{any|host dest_{host}_{address}\}\{eq dest_{port}|gt dest_{port}|lt dest_{port}|neq dest_{port}|range start dest_{port} end dest_{port}\}
```

**before**

```
before redirect css service \(svc_{name}[log]~\{tcp|udp\}\{eq|neq|lt|gt|range\} \{source_{address}|source_{wildcard}\}\{any|host source_{host}_{address}\}\{eq source_{port}|gt source_{port}|lt source_{port}|neq source_{port}|range start source_{port} end source_{port}\}\{dest_{address}|dest_{wildcard}\}\{any|host dest_{host}_{address}\}\{eq dest_{port}|gt dest_{port}|lt dest_{port}|neq dest_{port}|range start dest_{port} end dest_{port}\}
```

**after**

```
after redirect css service \(svc_{name}[log]~\{tcp|udp\}\{eq|neq|lt|gt|range\} \{source_{address}|source_{wildcard}\}\{any|host source_{host}_{address}\}\{eq source_{port}|gt source_{port}|lt source_{port}|neq source_{port}|range start source_{port} end source_{port}\}\{dest_{address}|dest_{wildcard}\}\{any|host dest_{host}_{address}\}\{eq dest_{port}|gt dest_{port}|lt dest_{port}|neq dest_{port}|range start dest_{port} end dest_{port}\}
```

**no redirect css service**

```
no redirect css service \(svc_{name}[log]~\{tcp|udp\}\{eq|neq|lt|gt|range\} \{source_{address}|source_{wildcard}\}\{any|host source_{host}_{address}\}\{eq source_{port}|gt source_{port}|lt source_{port}|neq source_{port}|range start source_{port} end source_{port}\}\{dest_{address}|dest_{wildcard}\}\{any|host dest_{host}_{address}\}\{eq dest_{port}|gt dest_{port}|lt dest_{port}|neq dest_{port}|range start dest_{port} end dest_{port}\}
```

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

**no**

Removes the rule definition which exactly matches the options specified.

---

**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`svc_name` must be a string from 1 through 15 characters in length.

---

**log**

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

---

**tcp | udp**

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

`tcp` : redirect applies to TPC packets.

`udp` : redirect applies to UDP packets.

---

**source_address**

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

---

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

---

**any**

Specifies that the rule definition applies to all packets.
**host**
Spefies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in dotted decimal notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

**range start_source_port end_source_port**
Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and end_source_port is the final port in the range.
Both start_source_port and end_source_port can be configured to any integer value from 0 to 65535.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

**dest_wildcard**
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

```
eq dest_port
```

Specifies a single, specific destination TCP port number to be filtered.  
`dest_port` must be configured to any integer value from 0 to 65535.

```
gt dest_port
```

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.  
`dest_port` must be configured to any integer value from 0 to 65535.

```
lt dest_port
```

Specifies that all destination TCP port numbers less than the one specified are to be filtered.  
`dest_port` must be configured to any integer value from 0 to 65535.

```
neq dest_port
```

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.  
`dest_port` must be configured to any integer value from 0 to 65535.

```
range start_dest_port end_dest_port
```

Specifies that all destination TCP ports within a specific range are to be filtered.  
`start_dest_port` is the initial port in the range and `end_dest_port` is the final port in the range.  
Both `start_dest_port` and `end_dest_port` can be configured to any integer value from 0 to 65535.

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named `chgsvc1`, and UDP packets coming from any host are matched.

```
redirect css service chgsvc1 udp any
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvc1 udp any
```

The following command sets the insertion point after the first rule definition above.

```
after redirect css service chgsvc1 udp any
```

The following deletes the rule definition above.

```
no redirect css service chgsvc1 udp any
```
redirect css service (for downlink, any)

Used to redirect subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction. This command is also used to set the access control list insertion point.

**Syntax**

```
redirect css service svc_name[ log]downlink any
before redirect css service svc_name[ log]downlink any
after redirect css service svc_name[ log]downlink any
no redirect css service svc_name[ log]downlink any
```

**Product**

All

**Privilege**

Security Administrator, Administrator

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**after**

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.

```
css service svc_name
```

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string from 1 through 15 characters in length.

```
downlink
```

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.
**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

---

**Usage**

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

---

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the *log* option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvlc* and any source IP.

```
redirect css service chgsvlc downlink any
```

The following sets the insertion point before the rule definition above.

```
before redirect service chgsvlc downlink any
```

The following command sets the insertion point after the first rule definition above.

```
after redirect service chgsvlc downlink any
```

The following deletes the first rule definition above.

```
no redirect service chgsvlc downlink any
```
redirect css service (for downlink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[
\text{redirect css service } \text{svc\_name} [ \text{log} ] \text{downlink host } \text{source\_host\_address} \\
\text{before redirect css service } \text{svc\_name} [ \text{log} ] \text{downlink host } \text{source\_host\_address} \\
\text{after redirect css service } \text{svc\_name} [ \text{log} ] \text{downlink host } \text{source\_host\_address} \\
\text{no redirect css service } \text{svc\_name} [ \text{log} ] \text{downlink host } \text{source\_host\_address} \\
\text{after} \\
\]

\[
\text{after} \\
\text{Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.} \\
\text{This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.} \\
\]

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

\[
\text{before} \\
\text{Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.} \\
\text{This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.} \\
\]

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

\[
\text{no} \\
\text{Removes the rule definition which exactly matches the options specified.} \\
\]

\[
\text{css service } \text{svc\_name} \\
\text{The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the show active-charging service all command to display the names of all configured charging services.} \\
\text{sdc\_name} \text{must be a string from 1 through 15 characters in length.} \\
\]

### ACL Configuration Mode Commands

**redirect css service (for downlink, by host IP address)**

**downlink**
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**host**
Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in dotted decimal notation.

### Usage
Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

### Important: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

### Example
The following command defines a rule definition that redirects packets to the charging service with the name `chgsvc`land a host IP address of `192.168.200.11`.

```
redirect service chgsvc1 downlink host 192.168.200.11
```

The following sets the insertion point before the rule definition above.

```
before redirect service chgsvc1 downlink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above.

```
after redirect service chgsvc1 downlink host 192.168.200.11
```

The following deletes the first rule definition above.

```
no redirect service chgsvc1 downlink host 192.168.200.11
```
redirect css service (for downlink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service svc_name[log]downlink icmp {any|host
source_host_address|source_address source_wildcard}{any|host
dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]
before redirect css service svc_name[log]downlink icmp {any|host
source_host_address|source_address source_wildcard}{any|host
dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]
after redirect css service svc_name[log]downlink icmp {any|host
source_host_address|source_address source_wildcard}{any|host
dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]
no redirect css service svc_name[log]downlink icmp {any|host
source_host_address|source_address source_wildcard}{any|host
dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]
```

important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

```
css service svc_name
```

The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source wildcard` parameter.

```
source_address
```

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

```
source wildcard
```

```
any
```

Specifies that the rule definition applies to all packets.

```
host
```

Specifies that the rule definition applies to a specific host as determined by its IP address.

```
source_host_address
```

The IP address of the source host to filter against expressed in dotted decimal notation.

```
dest_host_address
```

The IP address of the destination host to filter against expressed in dotted decimal notation.
ACL Configuration Mode Commands

redirect css service (for downlink, by ICMP packets)

**dest_address**
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

**dest_wildcard**
This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**icmp_type**
Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

**icmp_code**
Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**
Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service named `chgsvc1`, and ICMP packets coming in the downlink (from the Mobile Node) direction from the host with the IP address 198.162.100.25.

```
redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule definition above.

```
after redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following deletes the first rule definition above.
no redirect css service chgsvc1 downlink icmp host 192.168.100.25
redirect css service (for downlink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
redirect css service svc_name [log] downlink ip {any | host source_host_address | source_address source_wildcard} {any | host dest_host_address | dest_address dest_wildcard} [fragment] before redirect css service svc_name [log] downlink ip {any | host source_host_address | source_address source_wildcard} {any | host dest_host_address | dest_address dest_wildcard} [fragment] after redirect css service svc_name [log] downlink ip {any | host source_host_address | source_address source_wildcard} {any | host dest_host_address | dest_address dest_wildcard} [fragment] no redirect css service svc_name [log] downlink ip {any | host source_host_address | source_address source_wildcard} {any | host dest_host_address | dest_address dest_wildcard} [fragment]
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`svc_name` must be a string from 1 through 15 characters in length.

**downlink**

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule definition applies to all packets.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**destination_host_address**

The IP address of the destination host to filter against expressed in dotted decimal notation.
ACL Configuration Mode Commands

redirect css service (for downlink, by IP packets)

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**fragment**

Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**

Block IP packets when the source and destination are of interest.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and downlink IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched.

```
redirect css service chgsvc1 downlink ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvc1 downlink ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the first rule definition above.

```
after redirect css service chgsvc1 downlink ip host 198.162.100.25 any fragment
```

The following deletes the first rule definition above.

```
no redirect css service chgsvc1 downlink ip host 198.162.100.25 any fragment
```
redirect css service (for downlink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

`redirect css service svc_name[log]downlink source_address source_wildcard`
`before redirect css service svc_name[log]downlink source_address source_wildcard`
`after redirect css service svc_name[log]downlink source_address source_wildcard`
`no redirect css service svc_name[log]downlink source_address source_wildcard`

`after`
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

`before`
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

`no`
Removes the rule definition which exactly matches the options specified.

`css service svc_name`
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
**redirect css service** (for downlink, by source IP address masking)

- **svc_name** must be a string from 1 through 15 characters in length.

- **downlink**
  Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the filter are to be logged.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the **sourceWildcard** parameter.

- **sourceWildcard**
  This option is used in conjunction with the **source_address** option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**Usage**
Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Example**
The following command defines a rule definition to redirect packets to a charging service named **chgsvc1**. 
```
redirect css service chgsvc1 downlink 1.2.3.0 0.0.0.31
```
redirect css service (for downlink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service svc_name[log]downlink tcp udp \{ { source_address wildcard|any host source_host_address} \{ eq source_port|gt source_port|lt source_port|neq source_port|range start_source_port end_source_port \} \{ dest_address dest wildcard|any host dest_host_address \} \{ eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port \}
```

```
before redirect css service svc_name[log]downlink tcp udp \{ { source_address wildcard|any host source_host_address} \{ eq source_port|gt source_port|lt source_port|neq source_port|range start_source_port end_source_port \} \{ dest_address dest wildcard|any host dest_host_address \} \{ eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port \}
```

```
after redirect css service svc_name[log]downlink tcp udp \{ { source_address wildcard|any host source_host_address} \{ eq source_port|gt source_port|lt source_port|neq source_port|range start_source_port end_source_port \} \{ dest_address dest wildcard|any host dest_host_address \} \{ eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port \}
```

```
no redirect css service svc_name[log]downlink tcp udp \{ { source_address wildcard|any host source_host_address} \{ eq source_port|gt source_port|lt source_port|neq source_port|range start_source_port end_source_port \} \{ dest_address dest wildcard|any host dest_host_address \} \{ eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port \}
```

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```
before
```

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

**no**

Removes the rule definition which exactly matches the options specified.

---

**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string from 1 through 15 characters in length.

---

**downlink**

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

---

**log**

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

---

**tcp | udp**

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol. `tcp`: redirect applies to TPC packets. `udp`: redirect applies to UDP packets.

---

**source_address**

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

---

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.
any
Specifies that the rule definition applies to all packets.

host
Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in dotted decimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

range start_source_port end_source_port
Specifies that all source TCP ports within a specific range are to be filtered. 
start_source_port is the initial port in the range and end_source_port is the final port in the range. 
Both start_source_port and end_source_port can be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent. 
This option is used to filter all packets to a specific IP address or a group of IP addresses. 
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the destWildcard parameter.

dest wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. 
The mask must be entered as a complement:
ACL Configuration Mode Commands

redirect css service (for downlink, by TCP/UDP packets)

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**eq dest_port**
Specifies a single, specific destination TCP port number to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

**gt dest_port**
Specifies that all destination TCP port numbers greater than the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

**lt dest_port**
Specifies that all destination TCP port numbers less than the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

**neq dest_port**
Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

**range start_dest_port end_dest_port**
Specifies that all destination TCP ports within a specific range are to be filtered. `start_dest_port` is the initial port in the range and `end_dest_port` is the final port in the range. Both `start_dest_port` and `end_dest_port` can be configured to any integer value from 0 to 65535.

**Usage**
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service named `chgsvc1`, and UDP packets coming from any host are matched.
```
redirect css service chgsvc1 downlink udp any
```
The following sets the insertion point before the rule definition above.
```
before redirect css service chgsvc1 downlink udp any
```
The following command sets the insertion point after the first rule definition above.
```
after redirect css service chgsvc1 downlink udp any
```
The following deletes the rule definition above.
no redirect css service chgsvc1downlink udp any
redirect css service (for uplink, any)

Used to redirect subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
redirect css service svc_name [log] uplink any
before redirect css service svc_name [log] uplink any
after redirect css service svc_name [log] uplink any
no redirect css service svc_name [log] uplink any
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string from 1 through 15 characters in length.

**uplink**
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.
log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important: It is suggested that any rule definition which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important: A maximum of 16 rule definitions can be configured per ACL.

Important: Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule definition that redirects packets to the charging service with the name chgsvcl and any source IP.

```
redirect css service chgsvcl uplink any
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvcl uplink any
```

The following command sets the insertion point after the first rule definition above.

```
after redirect css service chgsvcl uplink any
```

The following deletes the first rule definition above.

```
no redirect css service chgsvcl uplink any
```
redirect css service (for uplink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name [log] uplink host source_host_address
before redirect css service svc_name [log] uplink host source_host_address
after redirect css service svc_name [log] uplink host source_host_address
no redirect css service svc_name [log] uplink host source_host_address
```

**uplink**
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
`svc_name` must be a string from 1 through 15 characters in length.
**ACL Configuration Mode Commands**

**redirect css service (for uplink, by host IP address)**

---

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

---

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

---

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `chgsvcl` and a host IP address of `192.168.200.11`.

```plaintext
redirect service chgsvcl uplink host 192.168.200.11
```

The following sets the insertion point before the rule definition above.

```plaintext
before redirect service chgsvcl uplink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above.

```plaintext
after redirect service chgsvcl uplink host 192.168.200.11
```

The following deletes the first rule definition above.

```plaintext
no redirect service chgsvcl uplink host 192.168.200.11
```
redirect css service (for uplink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name [log] uplink icmp [any | host source_host_address | source_address source_wildcard] [any | host dest_host_address | dest_address dest_wildcard] [icmp_type | icmp_code] before redirect css service svc_name [log] uplink icmp [any | host source_host_address | source_address source_wildcard] [any | host dest_host_address | dest_address dest_wildcard] [icmp_type | icmp_code]
```

```
after redirect css service svc_name [log] uplink icmp [any | host source_host_address | source_address source_wildcard] [any | host dest_host_address | dest_address dest_wildcard] [icmp_type | icmp_code]
```

```
no redirect css service svc_name [log] uplink icmp [any | host source_host_address | source_address source_wildcard] [any | host dest_host_address | dest_address dest_wildcard] [icmp_type | icmp_code]
```

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`svc_name` must be a string from 1 through 15 characters in length.

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule definition applies to all packets.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in dotted decimal notation.
ACL Configuration Mode Commands

**redirect css service (for uplink, by ICMP packets)**

`dest_address`

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `destWildcard` parameter.

`destWildcard`

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

`icmp_type`

Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

`icmp_code`

Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named `chgsvc1`, and ICMP packets in the uplink (to the Mobile Node) direction from the host with the IP address 198.162.100.25.

```
redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following sets the insertion point after the first rule definition above.

```
after redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following deletes the first rule definition above.

```
no redirect css service chgsvc1 uplink icmp host 192.168.100.25
```
redirect css service (for uplink, by ICMP packets)
redirect css service (for uplink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[log] uplink ip {any|host source_host_address|source_address source_wildcard} {any|host dest_host_address|dest_address dest_wildcard} [fragment]
before redirect css service svc_name[log] uplink ip {any|host source_host_address|source_address source_wildcard} {any|host dest_host_address|dest_address dest_wildcard} [fragment]
after redirect css service svc_name[log] uplink ip {any|host source_host_address|source_address source_wildcard} {any|host dest_host_address|dest_address dest_wildcard} [fragment]
no redirect css service svc_name[log] uplink ip {any|host source_host_address|source_address source_wildcard} {any|host dest_host_address|dest_address dest_wildcard} [fragment]
```

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string from 1 through 15 characters in length.

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule definition applies to all packets.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in dotted decimal notation.
redirect css service (for uplink, by IP packets)

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**fragment**

Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**

Block IP packets when the source and destination are of interest.

**Example**

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and uplink IP packets going to the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched.

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above.

```
before redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the first rule definition above.

```
after redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following deletes the first rule definition above.

```
no redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```
redirect css service (for uplink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[log] uplink source_address source_wildcard
before redirect css service svc_name[log] uplink source_address source_wildcard
after redirect css service svc_name[log] uplink source_address source_wildcard
no redirect css service svc_name[log] uplink source_address source_wildcard
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
`svc_name` must be a string from 1 through 15 characters in length.

**uplink**
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.
source_address

The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Example

The following command defines a rule definition to redirect packets to a charging service named chgsvc1.

```
redirect css service chgsvc1 uplink 1.2.3.0 0.0.0.31
```
**redirect css service (for uplink, by TCP/UDP packets)**

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[log] uplink {tcp|udp} {{ source_address source_wildcard|any|source_host_address}[eq source_port|gt source_port|lt source_port|neq source_port|range start_source_port end_source_port]} {{ dest_address dest_wildcard|any|host dest_host_address}[eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port]}
before redirect css service svc_name[log] uplink {tcp|udp} {{ source_address source_wildcard|any|host source_host_address}[eq source_port|lt source_port|range start_source_port end_source_port]} {{ dest_address dest_wildcard|any|host dest_host_address}[eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port]}
after redirect css service svc_name[log] uplink {tcp|udp} {{ source_address source_wildcard|any|host source_host_address}[eq source_port|gt source_port|lt source_port|range start_source_port end_source_port]} {{ dest_address dest_wildcard|any|host dest_host_address}[eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port]}
no redirect css service svc_name[log] uplink {tcp|udp} {{ source_address source_wildcard|any|host source_host_address}[eq source_port|gt source_port|lt source_port|range start_source_port end_source_port]} {{ dest_address dest_wildcard|any|host dest_host_address}[eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port end_dest_port]}
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**no**
Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string from 1 through 15 characters in length.

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**tcp | udp**

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol. `tcp`: redirect applies to TPC packets. `udp`: redirect applies to UDP packets.

**source_address**

The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**any**

Specifies that the rule definition applies to all packets.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in dotted decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in dotted decimal notation.
**eq source_port**
Specifies a single, specific source TCP port number to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**range start_source_port end_source_port**
Specifies that all source TCP ports within a specific range are to be filtered.
*start_source_port* is the initial port in the range and *end_source_port* is the final port in the range.
Both *start_source_port* and *end_source_port* can be configured to any integer value from 0 to 65535.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *destWildcard* parameter.

**destWildcard**
This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

**eq dest_port**
Specifies a single, specific destination TCP port number to be filtered.
*dest_port* must be configured to any integer value from 0 to 65535.

**gt dest_port**
Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
*dest_port* must be configured to any integer value from 0 to 65535.
**It dest_port**
Specifies that all destination TCP port numbers less than the one specified are to be filtered. 
dest_port must be configured to any integer value from 0 to 65535.

**neq dest_port**
Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. 
dest_port must be configured to any integer value from 0 to 65535.

**range start_dest_port end_dest_port**
Specifies that all destination TCP ports within a specific range are to be filtered. 
start_dest_port is the initial port in the range and end_dest_port is the final port in the range. 
Both start_dest_port and end_dest_port can be configured to any integer value from 0 to 65535.

**Usage**
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Example**
The following command defines a rule definition that redirects packets to the charging service named chgsvc1, and UDP packets coming from any host are matched.

```
redirect css service chgsvc1 uplink udp any
```
The following sets the insertion point before the rule definition above.
```
before redirect css service chgsvc1 uplink udp any
```
The following command sets the insertion point after the first rule definition above.
```
after redirect css service chgsvc1 uplink udp any
```
The following deletes the rule definition above.
```
no redirect css service chgsvc1 uplink udp any
```
redirect nexthop

The following commands redirect subscriber sessions to a nexthop IP address based on various parameters:
redirect nexthop (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard

afterredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard

beforeredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard

noredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard
```

- **after**
  Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
  This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

- **Important**: If the options specified do not exactly match an existing rule, the insertion point does not change.

- **before**
  Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
  This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

- **Important**: If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **nexthop nexthop_addr**
  The directly connected IP address to which the IP packets are forwarded.
context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

interface interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alpha and/or numeric string from 1 to 79 characters in length.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

Usage
Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

Important: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
Example
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31.

```
redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point before the rule defined above.

```
before redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the first rule defined above.

```
after redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above.

```
no redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```
**redirect nexthop (any)**

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any
```

```
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any
```

```
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any
```

```
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**nexthop nexthop_addr**
The directly connected IP address to which the IP packets are forwarded.
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

The name of the logical interface to which the packets should be redirected. `interface_name` must be an alpha and/or numeric string from 1 to 79 characters in length.

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**
Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

**Important:** It is suggested that any rule which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and any source IP.
```
redirect nexthop 192.168.10.4 context 23 any
```
The following sets the insertion point before the rule defined above.
```
before redirect nexthop 192.168.10.4 context 23 any
```
The following command sets the insertion point after the first rule defined above.
```
after redirect nexthop 192.168.10.4 context 23 any
```
The following deletes the first rule defined above.
```
no redirect nexthop 192.168.10.4 context 23 any
```
redirect nexthop (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

```plaintext
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

```plaintext
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

```plaintext
noredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

```plaintext
noshop nexthop_addr
```
The directly connected IP address to which the IP packets are forwarded.
redirect nexthop (by host IP address)

context context_id
The context identification number of the context to which packets are redirected. At the executive mode
prompt, use the **show context all** command to display context names and context IDs.

interface interface_name
The name of the logical interface to which the packets should be redirected. **interface_name** must be an
alpha and/or numeric string from 1 to 79 characters in length.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.

Usage
Define a rule when a very specific remote host is to be blocked. In simplified networks where the access
controls need only block a few hosts, this command allows the rules to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is
to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more
information.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers
facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the
context ID of 23 and a host IP address of 192.168.200.11.

```
redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following sets the insertion point before the rule defined above.
```
before redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following command sets the insertion point after the first rule defined above.
```
after redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following deletes the first rule defined above.
```
no redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```
redirect nexthop (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dst_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

after redirect interface_namексp_addr nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dst_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dst_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dst_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
redirect nexthop (by source ICMP packets)

no
Removes the rule which exactly matches the options specified.

next-hop nexthop_addr
The directly connected IP address to which the IP packets are forwarded.

context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

interface interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alpha and/or numeric string from 1 to 79 characters in length.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the sourceWildcard parameter.

sourceWildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.
**dest_host_address**
The IP address of the destination host to filter against expressed in dotted decimal notation.

**dest_address**
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `destWildcard` parameter.

**destWildcard**
This option is used in conjunction with the `destAddress` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `destAddress` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `destAddress` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**icmp_type**
Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

**icmp_code**
Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**
Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25.

```
redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following sets the insertion point before the rule defined above.

```
before redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule defined above.

```
after redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following deletes the first rule defined above.

```
no redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```
**redirect nexthop (by IP packets)**

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
redirect nexthop (by IP packets)

no
Removes the rule which exactly matches the options specified.

nexthop nexthop_addr
The directly connected IP address to which the IP packets are forwarded.

context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

interface interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alpha and/or numeric string from 1 to 79 characters in length.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.
**dest_host_address**
The IP address of the destination host to filter against expressed in dotted decimal notation.

**dest_address**
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**
This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.3, 0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**fragment**
Indicates packet redirection is to be applied to IP packet fragments only.

**protocol num**
Indicates that the packet filtering is to be applied to a specific protocol number. **num** can be any integer ranging from 0 to 255.

**Usage**
Block IP packets when the source and destination are of interest.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched.

```
redirect nexthop 192.168.10.4 context 23 ip host 198.162.100.25 any fragment
```
The following sets the insertion point before the rule defined above.

**before redirect next-hop 192.168.10.4 context 23 ip host 198.162.100.25 any fragment**

The following command sets the insertion point after the first rule defined above.

**after redirect next-hop 192.168.10.4 context 23 ip host 198.162.100.25 any fragment**

The following deletes the first rule defined above.

**no redirect next-hop 192.168.10.4 context 23 ip host 198.162.100.25 any fragment**
redirect nexthop (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address sourceWildcard | any | hostsource_host_address | eqsource_port | gtsource_port | ltsource_port | neqsource_port } { { dest_address destWildcard | any | hostdest_host_address | eqdest_port | gtdest_port | ltdest_port | negdst_port } }
```

```
afterredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address sourceWildcard | any | hostsource_host_address | eqsource_port | gtsource_port | ltsource_port | neqsource_port } { { dest_address destWildcard | any | hostdest_host_address | eqdest_port | gtdest_port | ltdest_port | negdst_port } }
```

```
beforeredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address sourceWildcard | any | hostsource_host_address | eqsource_port | gtsource_port | ltsource_port | neqsource_port } { { dest_address destWildcard | any | hostdest_host_address | eqdest_port | gtdest_port | ltdest_port | negdst_port } }
```

```
noredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address sourceWildcard | any | hostsource_host_address | eqsource_port | gtsource_port | ltsource_port | neqsource_port } { { dest_address destWildcard | any | hostdest_host_address | eqdest_port | gtdest_port | ltdest_port | negdst_port } }
```

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
ACL Configuration Mode Commands

**redirect nexthop (by TCP/UDP packets)**

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **nexthop** `nexthop_addr`
  The directly connected IP address to which the IP packets are forwarded.

- **context** `context_id`
  The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

- **interface** `interface_name`
  The name of the logical interface to which the packets should be redirected. `interface_name` must be an alpha and/or numeric string from 1 to 79 characters in length.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **tcp | udp**
  Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
  **tcp:** redirect applies to TPC packets.
  **udp:** redirect applies to UDP packets.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the **source wildcard** parameter.

- **source wildcard**
  This option is used in conjunction with the **source_address** option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.
any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in dotted decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in dotted decimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

lt source_port
 Specifies that all source TCP port numbers less than the one specified are to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

neq source_port
 Specifies that all source TCP port numbers not equal to the one specified are to be filtered. 
source_port must be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent. 
This option is used to filter all packets to a specific IP address or a group of IP addresses. 
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. 
The mask must be entered as a complement:
  ● Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical. 
  ● One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

### eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
*dest_port* must be configured to any integer value from 0 to 65535.

### gt dest_port
Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
*dest_port* must be configured to any integer value from 0 to 65535.

### lt dest_port
Specifies that all destination TCP port numbers less than the one specified are to be filtered.
*dest_port* must be configured to any integer value from 0 to 65535.

### neq dest_port
Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
*dest_port* must be configured to any integer value from 0 to 65535.

**Usage**
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and UDP packets coming from any host are matched.

```
redirect next hop 192.168.10.4 context 23 udp any
```
The following sets the insertion point before the rule defined above.

```
before redirect next hop 192.168.10.4 context 23 udp any
```
The following command sets the insertion point after the first rule defined above.

```
after redirect next hop 192.168.10.4 context 23 udp any
```
The following deletes the first rule defined above.

```
no redirect next hop 192.168.10.4 context 23 udp any
```
Chapter 6
ACS Group-of-Prefixed-URLs Configuration Mode

Commands

The Active Charging Service (ACS) Group-of-Prefixed-URLs Configuration Mode is used to create and configure ACS Group of Prefixed URLs.

Important: This configuration mode is customer specific. For more information, please contact your local service representative.

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

This command returns the CLI prompt to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`end`

**Usage**

Use this command to change to the Exec mode.
exit

This command exits the Group-of-Prefixed-URLs Configuration mode and returns to the Active Charging Service Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the Active Charging Service Configuration mode.
**prefixed-url**

This command configures the URLs to be filtered.

---

**Important:** A maximum of 10 URL filters can be configured per group.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] prefixed-url url
```

- **no**
  
  Removes the specified URL.

- **url**
  
  Specifies the URL, and must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

Use this command to configure the URLs to be filtered.

**Example**

The following command configures the URL `http://abc.net`:

```
prefixed-url http://abc.net
```
Chapter 7
ACS Host Pool Configuration Mode Commands

The ACS Host Pool Configuration Mode is used to define pool of host addresses and names within the ACS Configuration Mode. The Host Pool Configuration facilitates to create rules to handle the packets coming from or going to a group of hosts within an access policy.

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

This command exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to change to the Exec mode.
exit

This command exits the current configuration mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

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

This command specifies an individual or a range of host IP address(es) to add to the host pool.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ip { ip_address | ip_address/maskbit | range start_ip to end_ip }
```

- **no**
  Removes the specified IP address(es) that were configured previously from this host pool.

- **ip_address**
  Specifies an individual host IP address to add to this host pool.
  ip_address is the IP address in dotted decimal notation for IPv4 and in colon notation for IPv6.

- **ip_address/maskbit**
  Specifies an individual host IP address with subnet mask bit to add to this host pool.
  ip_address/maskbit is the IP address in dotted decimal notation for IPv4, and in colon notation for IPv6 with subnet mask bit. The maskbit is a numeric value which is the number of bits in the subnet mask.

- **range start_ip to end_ip**
  Specifies a range of host IP addresses to add to this host pool.
  start_ip is the start IP address of the range in dotted decimal notation for IPv4 and in colon notation for IPv6, and must be less than end_ip.
  end_ip is the end IP address of range in dotted decimal notation for IPv4 and in colon notation for IPv6, and must be greater than start_ip.

**Usage**

Use this command to add an individual or range of IP addresses to the host pool. Up to 10 sets of IP addresses can be configured in each host pool.

**Example**
The following command adds all IP addresses from 1.2.3.4 through 1.4.5.6 in IPv4 notation to the host pool:

```
ip range 1.2.3.4 to 1.4.5.6
```
Chapter 8
ACS IMSI Pool Configuration Mode Commands

The ACS IMSI Pool Configuration Mode is used to define pool of subscriber’s International Mobile Station Identifier numbers within the ACS Configuration Mode. IMSI pool configuration facilitates creation of rules to handle the packets coming from or going to a group of subscriber of IMSI numbers within an access policy.

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

This command exits the current configuration mode and returns to the Executive mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to change to the Executive mode.
exit

This command exits the current configuration mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

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

This command specifies an individual or a range of subscriber IMSI numbers to add to the IMSI pool.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[
\text{[ no ] imsi \{ imsi\_num | range \ start\_imsi \ to \ end\_imsi \}}
\]

no
Removes the specified subscriber IMSI number(s) that were configured previously from this IMSI pool.

\text{imsi\_num}
Specifies an individual subscriber IMSI number to add to this IMSI pool. \text{imsi\_num} is the IMSI number, and must be a sequence of hexadecimal digits between 1 and 15.

\text{range \ start\_imsi \ to \ end\_imsi}
Specifies a range of subscriber IMSI numbers to add to this IMSI pool. \text{start\_imsi} must be a sequence of hexadecimal numbers between 1 and 15 digits. This is the start IMSI number of subscriber IMSI range and must be less than \text{end\_imsi}. \text{end\_imsi} must be a sequence of hexadecimal numbers between 1 and 15 digits. This is the end IMSI number of subscriber IMSI range and must be greater than \text{start\_imsi}.

Usage
Use this command to specify the individual or range of subscriber IMSI numbers in an IMSI pool. Up to 10 sets of IMSI numbers can be configured in each IMSI pool.

Example
The following command adds the specified range of IMSI numbers to the IMSI pool:

\text{imsi range <start\_imsi> to <end\_imsi>}

Chapter 9
ACS Packet Filter Configuration Mode Commands

The Active Charging Service (ACS) Packet Filter Configuration Mode is used to create and configure ACS packet filters.

```
Exec Mode

active-charging
service name

ACS Configuration Mode

packet-filter
name

Packet Filter Configuration Mode
```

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

This command configures the direction in which the filter has to be applied.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Syntax**

direction { bi-directional | downlink | uplink }

default direction

default
Applies the default configuration.
Default: bi-directional

bi-directional
Specifies that the filter is to be applied in both uplink and downlink directions.

downlink
Specifies that the filter is to be applied in only downlink direction.

uplink
Specifies that the filter is to be applied in only uplink direction.

**Usage**
Use this command to configure the direction in which the filter has to be applied.

**Example**
The following command configures the filter in the downlink direction:

direction downlink
end

This command returns the CLI prompt to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to change to the Exec mode.
exit

This command exits the Packet Filter Configuration mode and returns to the Active Charging Service Configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the Active Charging Service Configuration mode.
ip local-port

This command configures the IP 5-tuple local port setting.

Product
ACS

Privilege
Security Administrator, Administrator

Syntax

    ip local-port { = port_number | range start_port_number to end_port_number }
    no ip local-port

    no
    Removes the local-port configuration, if previously configured.

    = port_number
    Specifies the port number of the transport protocol.
    port_number must be the port number, and must be an integer from 1 through 65535.

    range start_port_number to end_port_number
    range specifies a range of port numbers.
    start_port_number and end_port_number must be integers from 1 through 65535.
    end_port_number must be greater than start_port_number.

Usage
Use this command to configure a specific or range of IP local port setting for a packet filter.

Example
The following command configures the IP local port as 456:

    ip local-port = 456
ip protocol

This command configures the IP protocol setting.

Product
ACS

Privilege
Security Administrator, Administrator

Syntax

```
ip protocol { = protocol_number | range start_protocol_number to end_protocol_number }
```

```
no ip protocol
```

- `no`
  Removes the IP protocol configuration, if previously configured.

- `= protocol_number`
  Specifies the transport protocol field in the IP header. `protocol_number` must be the numerical value of the protocol, and must be an integer from 1 through 255.

- `range start_protocol_number to end_protocol_number`
  Specifies a range of protocol assignment numbers. `start_protocol_number` and `end_protocol_number` must be integers from 1 through 255. `end_protocol_number` must be greater than `start_protocol_number`.

**Important:** In StarOS 9.0 and later releases this keyword is obsolete.

Usage
Use this command to configure the protocol setting for a packet filter.

Example
The following command configures the protocol assignment number 300:
```
ip protocol = 300
```
ip remote-address

This command configures the IP remote address setting.

Product
ACS

Privilege
Security Administrator, Administrator

Syntax

```plaintext
ip remote-address { = { ip_address | ip_address/mask } | range { ip_address | ip_address/mask } to { ip_address | ip_address/mask } }

no ip remote-address
```

**no**
Removes the remote address configuration, if previously configured.

```plaintext
= { ip_address | ip_address/mask }
```

*ip_address* specifies the IP address in IPv4 dotted decimal or IPv6 colon separated notation format.

*ip_address/mask* specifies the IP address in IPv4 dotted decimal or IPv6 colon separated notation format, and the number of subnet bits representing the subnet mask in shorthand.

```plaintext
range { start_ip_address | start_ip_address/mask } to { end_ip_address | end_ip_address/mask }
```

**Important:** In StarOS 9.0 and later releases this keyword is obsoleted.

*range* specifies a range of IP addresses.

*start_ip_address* and *end_ip_address* specify, for the range, the starting and ending IP address in IPv4 dotted decimal or IPv6 colon separated notation format. *end_ip_address* must be greater than

*start_ip_address.*

*start_ip_address/mask* and *end_ip_address/mask* specify, for the range, the starting and ending IP address in IPv4 dotted decimal or IPv6 colon separated notation format, and the number of subnet bits representing the subnet mask in shorthand. *end_ip_address/mask* must be greater than

*start_ip_address/mask.*

Usage
Use this command to configure the remote IP address setting for a packet filter.

Example
The following command configures the IP remote address as 1.2.3.4/24:

```
ip remote-address = 1.2.3.4/24
```
**ip remote-port**

This command configures the IP remote port setting.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
ip remote-port { = port_number | range start_port_number to end_port_number }

no ip remote-port
```

- **no**
  Removes the remote port configuration, if previously configured.

- **= port_number**
  Specifies port number of the transport protocol.
  `port_number` must be the port number, and must be an integer from 1 through 65535.

- **range start_port_number to end_port_number**
  Specifies a range of port numbers.
  `start_port_number` and `end_port_number` must be integers from 1 through 65535.
  `end_port_number` must be greater than `start_port_number`.

**Usage**

Use this command to configure a specific or range of IP remote port settings for a packet filter.

**Example**

The following command configures the IP remote port as 789:

```bash
ip remote-port = 789
```
priority

This command configures the packet filter’s priority.

Product
ACS

Privilege
Security Administrator, Administrator

Syntax

```
priority priority
no priority
```

**Usage**

Use this command to configure the packet filter’s priority. Without this setting, this filter will not be used.

**Example**

The following command configures the packet filter’s priority as 3:

```
priority 3
```
Chapter 10
ACS Port Map Configuration Mode Commands

The ACS Port Map Configuration Mode is used to define application-port map in the ACS Configuration Mode. The application-port map facilitates to associate a range of port to specific application/protocol within a rule definition (ruledef).

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

This command exits the current configuration mode and returns to the Executive mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to change to the Executive mode.
exit

This command exits the current configuration mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

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

This command specifies a range of ports for application or protocol in ACS Port Map Configuration Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] port { port_num | range start_port to end_port }

no
Removes the specified port(s) / range of ports that were configured previously from this port map.

port_num
Specifies the port number to add to the port map.
port_num must be an integer from 1 through 65535.

range start_port to end_port
Specifies the range of ports for an application/protocol to add to this port map.
start_port must be an integer from 1 through 65535, and must be lesser than end_port.
end_port must be an integer from 1 through 65535, and must be greater than start_port.

Usage
Use this command to specify mapping between application and range of ports. Up to 10 sets of ports can be configured in each port map.

Example
The following command adds all ports from 3112 through 5000 to the port map:

port range 3112 to 5000
Chapter 11
Active Charging Service Configuration Mode Commands

The Active Charging Service (ACS) Configuration Mode is used to manage active charging service configurations. ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.

```
Exec Mode
  active-charging service name
    ACS Configuration Mode
```

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

This command enables creating/configuring/deleting access ruledefs.

**Important:** This command is only available in StarOS 8.1, and must be used to configure the Policy-based Stateful Firewall and NAT features.

<table>
<thead>
<tr>
<th>Product</th>
<th>FW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax**

```
access-ruledef ruledef_name [ -noconfirm ]
```

```
no access-ruledef ruledef_name
```

- **no**
  - Removes the specified access ruledef.

- **ruledef_name**
  - Specifies the access ruledef name.
  - `ruledef_name` must be a string of 1 through 63 characters in length, and can contain punctuation characters.
  - If the named access ruledef does not exist, it is created, and the CLI mode changes to the Firewall Ruledef Configuration Mode wherein the ruledef can be configured.
  - If the named access ruledef already exists, the CLI mode changes to the Firewall Ruledef Configuration Mode wherein the ruledef can be configured.

- **-noconfirm**
  - Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete an access ruledef. A ruledef contains different conditions/criteria to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique within the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.

**Important:** An access ruledef can be referenced by multiple firewall rulebases.

**Important:** The access ruledefs are different from the ACS ruledefs.
Example
The following command creates an access ruledef named `ruledef1`, and enters the Firewall Ruledef Configuration Mode:

```
firewall ruledef ruledef1
```
**bandwidth-policy**

This command enables creating/configuring/deleting a bandwidth policy.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bandwidth-policy policy_name [ -noconfirm ]
no bandwidth-policy policy_name
```

- **no**
  Removes the specified bandwidth policy.

- **policy_name**
  Specifies the bandwidth policy name. `policy_name` and must be an alpha and/or numeric string of 1 through 63 characters in length. If the named bandwidth policy does not exist, it is created, and the CLI mode changes to the Bandwidth Policy Configuration Mode wherein the bandwidth policy can be configured. If the named bandwidth policy already exists, the CLI mode changes to the Bandwidth Policy Configuration Mode wherein the bandwidth policy can be configured.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a bandwidth policy.

**Example**

The following command creates a bandwidth policy named `test73`, and enters the Bandwidth Policy Configuration mode:

```
bandwidth-policy test73
```
buffering-limit

This command sets the flow- or session-based packet buffering configuration.

Product

ECS

Privilege

Security Administrator, Administrator

Syntax

buffering-limit { flow-max-packets number | subscriber-max-packets number }
{ default | no } buffering-limit { flow-max-packets | subscriber-max-packets }

default
Sets the default value for the specified buffering limit configuration.
Default: no limit, other than the maximum amount of available memory

no
Removes the specified buffering limit configuration.

flow-max-packets number
Specifies the maximum number of packets that can be buffered per flow.
number must be an integer from 1 through 255.

subscriber-max-packets number
Specifies the maximum number of packets that can be buffered per subscriber.
number must be an integer from 1 through 255.

Usage

Use this command to configure the limits for buffering packets sent by a subscriber, while it is waiting for a response from the Diameter server. Packets need to be buffered for various reasons, such as, waiting for Credit Control Authorization or waiting for the result of a content filtering rating request.

Example

The following command sets the buffering limit per flow to 55:

buffering-limit flow-max-packets 55
charging-action

This command enables creating/configuring/deleting a charging action in the current Active Charging Service.

**Important:** A maximum of 2048 charging actions can be configured in an Active Charging Service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] charging-action charging_action_name [ -noconfirm ]
```

- **no**
  Removes the specified charging action.

- **charging_action_name**
  Specifies the charging action name.
  `charging_action_name` must be an alpha and/or numeric string of 1 through 63 characters in length, and can contain punctuation characters.
  If the named charging action does not exist, it is created, and the CLI mode changes to the Charging Action Configuration Mode wherein the charging action can be configured.
  If the named charging action already exists, the CLI mode changes to the Charging Action Configuration mode wherein the charging action can be configured.
  The charging action name must be unique for a given Active Charging Service. Up to 2048 charging actions can be configured in a system across all Active Charging services.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a charging action in the current Active Charging Service.
A charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (e.g., an EDR) to dropping the IP packet, etc. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3/L4/L7 etc).

**Example**
The following command creates a charging action named `action123`:

```
charging-action action123
```
content-filtering category match-method

This command sets the match method to look up URLs in the Category-based Content Filtering database.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ccontent-filtering category match-method { exact | generic }
default content-filtering category match-method
```

- **default**
  Sets the default match method.
  Default: Generic

- **exact**
  Specifies the exact-match method, wherein URLs are rated only on exact match with URLs present in the Category-based Content Filtering database.

- **generic**
  Specifies the generic-match method, wherein normalization, multi-lookups, rollback algorithms are applied to URLs during look up, and URLs are rated on generic match with URLs present in the Category-based Content Filtering database.

**Usage**
Use this command to set the match method to look up URLs in the Category-based Content Filtering database.

**Example**
The following command sets the exact-match method to look up URLs in the Category-based Content Filtering database:

```
ccontent-filtering category match-method exact
```
content-filtering category policy-id

This command enables creating/configuring/deleting Content Filtering Category Policies for Category-based Content Filtering support.

**Important:** A maximum of 64 Content Filtering Category Policies can be configured in an Active Charging Service.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
content-filtering category policy-id cf_policy_id [ description [ description_string ] ] [ -noconfirm ]
```

```plaintext
no content-filtering category policy-id cf_policy_id
```

- **no**
  Deletes the specified Content Filtering Category Policy.

- **category policy-id cf_policy_id**
  Specifies the Content Filtering Category Policy ID.
  *cf_policy_id* must be an integer from 1 through 4,294,967,295.
  If the specified policy ID does not exist, it is created and the CLI mode changes to the Content Filtering Policy Configuration mode, wherein the policy can be configured.
  If the specified policy ID already exists, the CLI mode changes to the Content Filtering Policy Configuration mode, wherein the policy can be configured.

- **description [ description_string ]**
  Specifies a description for the Content Filtering Category Policy.
  *description_string* must be a string of 1 through 31 characters in length.
  Note that both *description* and *description_string* are optional.
  “*description*” saves *description_string* as the new description.
  “*description*” removes the previously specified description.
  This description is displayed in the output of the “show content-filtering category policy-id id” and “show active-charging service name service_name” commands.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a Content Filtering Category Policy.
Example
The following command creates a Content Filtering Policy with the ID 101, and enters the Content Filtering Policy Configuration mode:

```
content-filtering category policy-id 101
```
credit-control

This command enables/disables Prepaid Credit Control Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] credit-control [ group group_name ]

no
Disables Prepaid Credit Control Application configuration.

group group_name

Important: The group keyword is only available in StarOS 8.1 and later releases.

Specifies the credit control group name.
group_name must be an alpha and/or numeric string of 1 through 63 characters in length.
If the named credit control group does not exist, it is created, and the CLI mode changes to the Credit Control Configuration mode, wherein the credit control group can be configured.
If the named credit control group already exists, the CLI mode changes to the Credit Control Configuration mode, wherein the credit control group can be configured.
Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.
Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.

Usage

Use this command to enable/disable Prepaid Credit Control Configuration for RADIUS/Diameter charging mode.

Example

The following command enables prepaid credit control accounting to use RADIUS and/or Diameter interface mode.
credit-control
diameter credit-control

**Description** This command has been obsoleted, and is replaced by the `credit-control` command.
edr-format

This command enables creating/configuring/deleting an EDR format specification for the current Active Charging Service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
edr-format name [ -noconfirm ]
```

```
no edr-format name
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified EDR format from the current Active Charging Service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the EDR format name.</td>
</tr>
</tbody>
</table>

`name` must be a string of 1 through 63 characters in length.
If the named EDR format does not exist, it is created, and the CLI mode changes to the EDR Format Configuration Mode wherein the EDR format can be configured.
If the named EDR format already exists, the CLI mode changes to the EDR Format Configuration mode wherein the EDR format can be configured.
The EDR format name must be unique for a given Active Charging Service. Up to 256 combined total EDR plus UDR formats can be configured in a system across all Active Charging Services.

<table>
<thead>
<tr>
<th><strong>-noconfirm</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the command must execute without prompting for confirmation.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to create/configure/delete an EDR format for a specified Active Charging Service.

**Example**
The following command creates an EDR format named `edr_format1`:

```
edr-format edr_format1
```
edr-udr-flow-control

This command enables Flow Control between Session Managers and the CDRMOD process.

Product
All

Privilege
Security Administrator, Administrator

Syntax

edr-udr-flow-control [ unsent-queue-size queue_size ]
{ default | no } edr-udr-flow-control

no
Disables Flow Control.

default
Configures the default setting.
Default: Flow Control is enabled; unsent-queue-size is set to 375

unsent-queue-size queue_size
Specifies the Flow Control unsent queue size at sessmgr level.
queue_size must be an integer from 1 through 2500.

Usage
Use this command to enable Flow Control between Session Managers and the CDRMOD process, and configure the unsent queue size.

Example
The following command enable Flow Control between Session Managers and the CDRMOD process, and configure the unsent queue size to 1000:

    edr-udr-flow-control unsent-queue-size 1000
end

This command returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
exit

This command exits the Active Charging Service Configuration mode and returns to the Global Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the Global Configuration mode.
fair-usage

This command enables Fair Usage feature configuration.

**Product**
ECS, CF, FW, NAT, P2P

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
fair-usage [ deact-margin deactivate_margin | threshold-percent usage_threshold ]
default fair-usage [ deact-margin | threshold-percent ]
```

**default**
Configures the default Fair Usage monitoring settings.
Default:
- `deact-margin`: 5 percent
- `threshold-percent`: 50 percent

**deact-margin deactivate_margin**
Specifies that Fair Usage monitoring must be disabled when the instance-level credit usage goes `deactivate_margin` percentage below `usage_threshold`.
`deactivate_margin` is a percentage value, and must be an integer from 1 through 100.

**threshold-percent usage_threshold**
Specifies the threshold to start Fair Usage monitoring. Till the credit usage hits this threshold, all session resource allocation is allowed. On crossing this threshold, any new resource allocation request is evaluated and allowed or failed.
`usage_threshold` is a percentage value, and must be an integer from 1 through 100.

**Usage**
Use this command to enable the Fair Usage feature, which enables to perform SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

**Example**
The following command enables the Fair Usage feature, and configures the session resource usage threshold to start Fair Usage monitoring to 75%:

```plaintext
fair-usage threshold-percent 75
```

The following command configures the deactivate margin to disable Fair Usage monitoring to 10% below the session resource usage threshold (65%):

```plaintext
fair-usage deact-margin 10
```
## firewall dos-protection

This command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.

### Important:
In StarOS 8.1 and later, for Rulebase-based Stateful Firewall this command is available in the Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the Rulebase Configuration Mode.

### Product
FW

### Privilege
Security Administrator, Administrator

### Syntax

```
[ no ] firewall dos-protection { all | flooding ( icmp | tcp-syn | udp ) | ftp-bounce | ip-unaligned-timestamp | mime-flood | seq-number-out-of-range | seq-number-prediction | source-router | teardrop | winnukes }
```

### default firewall dos-protection

```
no
```

Disables protection for subscribers from the specified DoS attack(s).

```
default
```

Sets Stateful Firewall DOS protection to the default setting.

```
all
```

Enables protection against all DoS attacks supported by Stateful Firewall.

```
flooding { icmp | tcp-syn | udp }
```

Enables protection against specified flooding attacks:

- `icmp`: Enables protection against ICMP Flood attack
- `tcp-syn`: Enables protection against TCP Syn Flood attack
- `udp`: Enables protection against UDP Flood attack

```
ftp-bounce
```

Enables protection against FTP bounce attacks.

```
ip-unaligned-timestamp
```

Enables protection against IP unaligned timestamp attacks.

```
mime-flood
```

Enables protection against Multiple Internet Mail Extension (MIME) header flooding attacks.
### seq-number-out-of-range
Enables protection against an out of range sequence attacks.

### seq-number-prediction
Enables protection against TCP sequence prediction attacks.

### source-router
Enables protection against attacks caused by loose source routing.

### teardrop
Enables protection against Teardrop attacks.

### winnuke
Enables protection against WIN-NUKE attacks.

---

#### Usage
Use this command to enable the Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

#### Example
The following command enables protection from all DoS attacks supported by the Stateful Firewall:

```bash
firewall dos-protection all
```
firewall flooding

This command configures Stateful Firewall protection from packet flooding attacks.

**Important:** In StarOS 8.1 and later, for Rulebase-based Stateful Firewall this command is available in the Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the Rulebase Configuration Mode.

### Product
FW

### Privilege
Security Administrator, Administrator

### Syntax
```
firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit packets } | { sampling-interval interval } }

default firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit } | { sampling-interval } }
```

- `default`
  - Sets the specified firewall flooding configuration to the default value.

- `protocol { icmp | tcp-syn | udp }`
  - Specifies the transport protocol:
    - `icmp`: Configuration for ICMP protocol.
    - `tcp-syn`: Configuration for TCP-SYN packet limit.
    - `udp`: Configuration for UDP protocol.

- `packet limit packets`
  - Specifies the maximum number of specified packets a subscriber can receive during a sampling interval. `packets` is the maximum number of packets allowed during a sampling interval, and must be an integer from 1 through 4294967295.
  - Default: 1000 packets per sampling-interval.

- `sampling-interval interval`
  - Specifies the flooding sampling interval in seconds.
  - `interval` must be an integer from 1 through 60.
  - Default: 1 second
  - The maximum sampling-interval configurable is 60 seconds.

### Usage
Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.
Example
The following command ensures a subscriber will not receive more that 1000 ICMP packets per sampling interval:

```bash
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IPs, those packets will be limited to 1000 packets per sampling interval. This way only “suspected” malicious packets are limited and not “legitimate” packets.

```bash
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 TCP-Syn packets per sampling interval.

```bash
firewall flooding protocol tcp-syn packet limit 1000
```

The following command specifies a flooding sampling interval of 1 second:

```bash
firewall flooding sampling-interval 1
```
firewall flow-recovery

This command configures Stateful Firewall Flow Recovery settings.

Product
FW

Privilege
Security Administrator, Administrator

Syntax

firewall flow-recovery { { downlink [ [ timeout timeout ] [ no-flow-creation ] ] } | { uplink [ timeout timeout ] } } }

{ default | no } firewall flow-recovery { downlink | uplink }

default
Configures the default setting.
Default: downlink and uplink recovery is enabled, 300 seconds

no
Disables the previous configuration.

downlink | uplink
Specifies the packets:
downlink: Enables flow recovery for packets from downlink direction.
uplink: Enable flow recovery for packets from uplink direction.

timeout timeout
Specifies the Stateful Firewall Flow Recovery Timeout setting, in seconds.
timeout must be an integer from 1 through 86400.
Default: 300 seconds

no-flow-creation
Specifies not to create data session/flow-related information for downlink-initiated packets (from the Internet to the subscriber) while the firewall downlink flow-recovery timer is running, but send to subscriber.

Usage
Use this command to configure Stateful Firewall Flow Recovery.

Important: NAT flows will not be recovered.

Example
The following command configures Stateful Firewall Flow Recovery for packets in downlink direction with a timeout of 600 seconds:

```
firwall flow-recovery downlink timeout 600
```
**firewall icmp-destination-unreachable-message-threshold**

This command configures a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.

> **Important:** In StarOS 8.1 and later, for Rulebase-based Stateful Firewall this command is available in the Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the Rulebase Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall icmp-destination-unreachable-message-threshold messages then-block-server
{ default | no } firewall icmp-destination-unreachable-message-threshold
```

**Usage**

Use this command to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked. Some servers that run QChat ignore the ICMP error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive the unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.

**Example**

The following command configures a threshold of 10 ICMP error messages:

```
firewall icmp-destination-unreachable-message-threshold 10 then-block-server
```
firewall max-ip-packet-size

This command configures the maximum IP packet size allowed over Stateful Firewall.

**Important:** In StarOS 8.1 and later, for Rulebase-based Stateful Firewall this command is available in the Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the Rulebase Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall max-ip-packet-size packet_size protocol { icmp | non-icmp }
default firewall max-ip-packet-size protocol { icmp | non-icmp }
```

**default**
Sets the maximum IP packet size configuration to the default value.
Default: 65535 bytes (for both ICMP and non-ICMP)

**packet_size**
Specifies the maximum packet size.
`packet_size` must be an integer from 30000 through 65535.

**protocol { icmp | non-icmp }**
Specifies the transport protocol:
- `icmp`: Configuration for ICMP protocol.
- `non-icmp`: Configuration for protocols other than ICMP.

**Usage**
Use this command to configure the maximum IP packet size allowed for ICMP and non-ICMP packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for “Jolt Attack” and “Ping-Of-Death Attack”.

**Example**
The following command allows a maximum packet size of 60000 for ICMP protocol:
```
firewall max-ip-packet-size 60000 protocol icmp
```
firewall mime-flood

This command configures Stateful Firewall protection from mime-flood attacks.

**Important:** In StarOS 8.1 and later, for Rulebase-based Stateful Firewall this command is available in the Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the Rulebase Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall mime-flood { http-headers-limit max_limit | max-http-header-field-size max_size }

default firewall mime-flood { http-headers-limit | max-http-header-field-size }
```

**default**
Sets the specified firewall mime flood configuration to the default value.

**http-headers-limit max_limit**
Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.

*max_limit* must be an integer from 1 through 256.
Default: 16

**max-http-header-field-size max_size**
Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.

*max_size* must be an integer from 1 through 8192.
Default: 4096 bytes

**Usage**
Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent the mime flooding attacks.

**Example**
The following command sets the maximum number of headers allowed in an HTTP packet to 100:

```
firewall mime-flood http-headers-limit 100
```

The following command sets the maximum header field size allowed in the HTTP header to 1000 bytes:

```
firewall mime-flood max-http-header-field-size 1000
```
firewall nat-alg

This command enables/disables NAT Application Level Gateways (ALGs).

Product  
NAT

Privilege  
Security Administrator, Administrator

Syntax

[ default | no ] firewall nat-alg { all | ftp | pptp | rtsp | sip }

default
Configures the default setting.
Default:
• ftp: enabled
• pptp: disabled
• rtsp: disabled
• sip: disabled

no
Disables all/specified NAT ALG configuration. When disabled, the ALG(s) would not do any payload translation for NATd calls.

all | ftp | pptp | rtsp | sip
Specifies the NAT ALG to enable/disable.
• all: Enables/disables all of the following NAT ALGs.
• ftp: Enables/disables File Transfer Protocol (FTP) NAT ALG.
• pptp: Enables/disables Point-to-Point Tunneling Protocol (PPTP) NAT ALG.
• rtsp: Enables/disables Real Time Streaming Protocol (RTSP) ALG.
• sip: Enables/disables Session Initiation Protocol (SIP) NAT ALG.

Usage
Use this command to enable/disable NAT ALGs.
To enable NAT ALG processing, in addition to this configuration, ensure that the routing rule for that particular protocol is added in the rulebase.

Example
The following command enables FTP NAT ALG:

firewall nat-alg ftp

The following command disables FTP NAT ALG:

no firewall nat-alg ftp
The following command enables FTP NAT ALG, and disables PPTP, RTSP, SIP NAT ALGs:

default firewall nat-alg all
firewall no-ruledef-matches

This command configures the default action for packets when no firewall ruledef matches.

**Important:** In StarOS 8.1 and later releases, this command is available in the Rulebase Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall no-ruledef-matches { downlink | uplink } action { deny [ charging-action charging_action ] | permit }
```

**default firewall no-ruledef-matches { downlink | uplink } action**

default

Configures the default action for packets with no firewall ruledef match.
Default: uplink direction: permit, downlink direction: deny

downlink | uplink

Specifies the packet type:
downlink: Downlink packets with no firewall ruledef match.
uplink: Uplink packets with no firewall ruledef match.

**action { deny [ charging-action charging_action ] | permit }**

Specifies the default action for packets with no firewall ruledef match.

- **permit:** Permit specified packets.
- **deny [ charging-action charging_action ]:** Deny specified packets.
  Optionally, a charging action can be specified. charging_action must be the name of a charging action, and must be a string of 1 through 63 characters in length.

**Usage**

Use this command to configure the default action to be taken on packets with no firewall ruledef matches.
If, for deny action, the optional charging action is configured, the action taken depends on what is configured in the charging action. For the firewall rule, the “flow action”, “billing action”, and “content ID” of the charging action will be used to take action. If flow exists, flow statistics are updated.

**Example**
The following command sets Stateful Firewall to permit downlink packets with no ruledef matches:
```
firwall no-ruledef-matches downlink action permit
```
firewall port-scan

This command configures the Port Scan Detection algorithm.

Product
FW

Privilege
Security Administrator, Administrator

Syntax

firewall port-scan { connection-attempt-success-percentage { non-scanner | scanner } percentage | inactivity-timeout inactivity_timeout | protocol { tcp | udp } response-timeout response_timeout | scanner-policy { block inactivity-timeout | log-only } }

default firewall port-scan { connection-attempt-success-percentage { non-scanner | scanner } | inactivity-timeout | protocol { tcp | udp } response-timeout | scanner-policy }

default
Configures default parameters for port-scan detection.

connection-attempt-success-percentage { non-scanner | scanner } percentage
Specifies the connection attempt success percentage:
non-scanner: Specifies the connection attempt success percentage for a non-scanner. percentage must be an integer from 60 through 99.
Default: 70%
scanner: Specifies the connection attempt success percentage for a scanner. percentage must be an integer from 1 through 40.
Default: 30%

inactivity-timeout inactivity_timeout
Specifies the port scan inactivity timeout period, in seconds.
inactivity_timeout must be an integer from 60 through 1800.
Default: 300 seconds

protocol { tcp | udp } response-timeout response_timeout
Specifies transport protocol specific response timeout period:
tcp: Specifies response timeout for TCP. response_timeout must be an integer from 3 through 30.
udp: Specifies response timeout for UDP. response_timeout must be an integer from 3 through 60.
Default: 3 seconds

scanner-policy { block inactivity-timeout inactivity_timeout | log-only }
Specifies the scanner policy.
Default: Log only
block inactivity-timeout \texttt{inactivity\_timeout}: Specifies blocking any subsequent traffic from the scanner. If the scanner is found to be inactive for the inactivity-timeout period, then the scanner is no longer blocked, and traffic is allowed. 
\texttt{inactivity\_timeout} specifies the scanner inactivity timeout period, in seconds, and must be an integer from 1 through 4294967295.

\texttt{log-only}: Specifies logging scanner information without blocking scanner traffic.

\underline{Usage}

Use this command to configure the Port Scan Detection algorithm.

\underline{Example}

The following command configures the Stateful Firewall Port Scan inactivity timeout period to 900 seconds:
\texttt{firewall port-scan inactivity-timeout 900}
firewall ruledef

This command enables creating/configuring/deleting firewall ruledefs.

**Important:** This command is only available in StarOS 8.1, and is customer-specific. This command must be used to configure the Rulebase-based Stateful Firewall and NAT features.

### Product
FW

### Privilege
Security Administrator, Administrator

### Syntax

```
fwp ruledef ruledef_name [ -noconfirm ]
```

```
no firewall ruledef ruledef_name
```

---

**no**

Removes the specified firewall ruledef.

**ruledef_name**

Specifies the firewall ruledef name. 

*ruledef_name* must be a string of 1 through 63 characters in length, and can contain punctuation characters. 

If the named firewall ruledef does not exist, it is created, and the CLI mode changes to the Firewall Ruledef Configuration Mode wherein the ruledef can be configured. 

If the named firewall ruledef already exists, the CLI mode changes to the Firewall Ruledef Configuration Mode wherein the ruledef can be configured.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

---

**Usage**

Use this command to create/configure/delete a firewall ruledef. A firewall ruledef contains different conditions/criteria to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.

**Important:** A firewall ruledef can be referenced by multiple firewall rulebases.

**Important:** The firewall ruledefs are different from the Active Charging Ruledefs.
Example
The following command creates a firewall ruledef named `fw_ruledef1`, and enters the Firewall Ruledef Configuration Mode:

`firewall ruledef fw_ruledef1`
**firewall tcp-syn-flood-intercept**

This command enables and configures the TCP intercept parameters to prevent TCP-SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the `dos-protection` command.

⚠️ **Important:** In StarOS 8.1 and later, for Rulebase-based Stateful Firewall this command is available in the Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the Rulebase Configuration Mode.

### Syntax

```
firewall tcp-syn-flood-intercept { max-attempts max_attempts | mode { none | { intercept | watch } [ aggressive ] } | retrasm-timeout retrasm_timeout | watch-timeout intercept_watch_timeout }
```

```
default firewall tcp-syn-flood-intercept { max-attempts | mode | retrasm-timeout | watch-timeout }
```

### `default`

Sets the default values of TCP intercept parameters for SYN Flood DoS protection.

### `max-attempts max_attempts`

Default: 5

Specifies the maximum number of attempts for sending proxy SYN to the target. This keyword works in conjunction with the `retransmit-timeout` keyword.

`max_attempts` specifies the maximum number of attempts for sending proxy SYN to the target after the timeout duration, and must be an integer from 1 through 5.

### `mode { none | { intercept | watch } [ aggressive ]`

Default: `none`

Specifies TCP SYN flood intercept mode:

- **intercept**: Configures TCP SYN flood intercept feature in intercept mode.
- **none**: Disables TCP SYN flood intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. The Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, the Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in
watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus, the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

**retransmit-timeout** retransmit_timeout

Default: 60
Specifies the SYN-Proxy retransmit timeout in seconds. System waits for this period before sending proxy SYN to the target. This keyword works in conjunction with `max-attempts` keyword.
retransmit_timeout specifies the duration in seconds the system waits before sending proxy SYN, and must be an integer from 15 through 60.

**watch-timeout** intercept_watch_timeout

Default: 30
intercept_watch_timeout specifies the TCP intercept watch timeout in seconds, and must be an integer from 5 through 30.

**Usage**
This TCP intercept functionality provides protection against TCP SYN Flooding attacks. The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

**Example**
The following command sets the maximum number of attempts for sending proxy SYN to the target to 5:

```
firwall tcp-syn-flood-intercept max-attempts 5
```
firewall track-list

This command configures the maximum number of server IPs to be tracked that are involved in any kind of DOS attacks.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall track-list attacking-servers no_of_servers

{ default | no } firewall track-list attacking-servers
```

- **default**
  
  Sets the default configuration.
  
  Default: 10

- **no**

**Important:** This variant is only available in StarOS 8.3 and later releases.

**Usage**

Use this command to configure the maximum number of server IPs to be tracked that are involved in any kind of DOS attacks.

**Example**

The following command configures the maximum number of server IPs to be tracked that are involved in any kind of DOS attacks to 20:

```plaintext
firewall track-list attacking-servers 20
```
fw-and-nat policy

This command enables creating/configuring/deleting a Firewall-and-NAT policy.

**Important:** This command is only available in StarOS 8.1 and StarOS 9.0 and later releases. This command must be used to configure the Policy-based Stateful Firewall and NAT features.

**Product**
FW, NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
fw-and-nat policy policy_name [ -noconfirm ]
```

```
no fw-and-nat policy policy_name
```

- **no**
  Deletes the specified Firewall-and-NAT policy.

**Important:** When a Firewall-and-NAT policy is deleted, for all subscribers using the policy, Stateful Firewall and NAT processing is disabled, also ECS sessions for the subscribers are dropped. In case of session recovery, the calls are recovered but with Stateful Firewall and NAT disabled.

- **policy_name**
  Specifies the Firewall-and-NAT policy name.
  `policy_name` must be an alpha and/or numeric string of 1 through 63 characters in length.
  If the named Firewall-and-NAT policy does not exist, it is created and the CLI mode changes to the Firewall-and-NAT Policy Configuration mode, wherein the policy can be configured.
  If the named Firewall-and-NAT policy already exists, the CLI mode changes to the Firewall-and-NAT Policy Configuration mode, wherein the named policy can be configured.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a Firewall-and-NAT policy.

**Example**
The following command creates a Firewall-and-NAT policy named `test321`, and changes to the Firewall-and-NAT Policy Configuration Mode:

```
fw-and-nat policy test321
```
group-of-prefixed-urls

This command enables creating/configuring/deleting a group-of-prefixed-URLs.

**Important:** This command is customer specific. For more information, please contact your local sales representative.

**Important:** A maximum of 64 group-of-prefixed-URL groups can be configured in the Active Charging Service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
group-of-prefixed-urls group_name [ -noconfirm ]
```

```
no group-of-prefixed-urls group_name
```

**Usage**

Use this command to create/configure/delete a group of prefixed URLs.

**Example**

The following command creates group-of-prefixed-urls named `test5`, and enters the ACS Group of Prefixed URLs Configuration Mode:

```
group-of-prefixed-urls test5
```
(group-of-ruledefs)

This command enables creating/configuring/deleting a group-of-ruledefs.

**Important:** A maximum of 64 groups-of-ruledefs can be configured in an Active Charging Service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
group-of-ruledefs ruledef_group [ -noconfirm ]
```

```
no group-of-ruledefs ruledef_group
```

**Usage**
Use this command to create/configure/delete a group-of-ruledefs. A group-of-ruledefs is a collection of rule definitions to use in access policy creation. The group-of-ruledefs name must be unique within the service.

**Example**
The following command creates a group-of-ruledefs named **group1**, and enters the Group-of-Ruledefs Configuration Mode:

```
group-of-ruledefs group1
```
host-pool

This command enables creating/configuring/deleting a host pool.

Product
All

Privilege
Security Administrator, Administrator

Syntax

host-pool host_pool [ -noconfirm ]

no host-pool host_pool

no
Removes the specified host pool.

host_pool
Specifies the host pool name.
host_pool must be a string of 1 through 63 characters in length, and can contain punctuation characters.
If the named host pool does not exist, it is created, and the CLI mode changes to the ACS Host Pool Configuration Mode wherein the host pool can be configured.
If the named host pool already exists, the CLI mode changes to the ACS Host Pool Configuration Mode wherein the host pool can be configured.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete ACS host pools.
A host pool is a collection of hosts and IP addresses to use in access policy creation. The host pool name must be unique within the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 host pools can be created.

Important: Host pools in use in other ruledefs cannot be deleted.

Example

The following command creates a host pool named hostpool1, and enters the ACS Host Pool Configuration Mode:

host-pool hostpool1
idle-timeout

This command configures the maximum duration a flow can remain idle, in seconds, after which the system automatically terminates the flow.

**Product**
ECS, NAT, FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
idle-timeout { alg-media | icmp | tcp | udp } idle_timeout

{ default | no } idle-timeout { alg-media | icmp | tcp | udp }
```

- **default**
  Configures the default idle-timeout setting for the specified flow.
  Default: `alg-media`: 120 seconds; `icmp,tcp,udp`: 300 seconds

- **no**
  Disables the idle-timeout configuration for the specified flow.

- **alg-media | icmp | tcp | udp**
  Configures/disables the idle-timeout setting for the specified flow.

- **idle_timeout**
  Specifies the timeout duration, in seconds, and must be an integer from 0 through 86400.
  For `alg-media` specifies the media inactivity timeout. The `idle_timeout` value gets applied on RTP and RTCP media flows that are created for SIP/H.323 calls. The timeout is applied only on those flows that actually match the RTP and RTCP media pinholes that are created by the SIP/H.323 ALG.
  A value of 0 disables the idle-timeout setting.

**Usage**
Use this command to configure the maximum duration a flow can remain idle, in seconds, after which the system automatically terminates the flow.
Setting the value to 0 will cause the idle-timeout setting to be disabled.
For flows other than TCP, UDP, and ICMP timeout will always be 300 seconds. (Unless configured in the charging-action). Charging action’s flow idle-timeout will have precedence over ACS idle-timeout. If charging action’s flow idle-timeout is default, then flows will have the value configured in the ACS service.

**Example**
The following command configures the maximum duration a TCP flow can remain idle to 3000 seconds, after which the system automatically terminates the flow:

```
idle-timeout tcp 3000
```
**imsi-pool**

This command enables creating/configuring/deleting an IMSI pool.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

`imsi-pool  imsi_pool  [  -noconfirm  ]`

`no  imsi-pool  imsi_pool`

---

**Syntax**

`no`

Removes the specified IMSI pool.

`imsi_pool`

Specifies the IMSI pool name.

`imsi_pool` must be a string of 1 through 63 characters in length, and can contain punctuation characters.

If the named IMSI pool does not exist, it is created, and the CLI mode changes to the ACS IMSI Pool Configuration Mode wherein the IMSI pool can be configured.

If the named IMSI pool already exists, the CLI mode changes to the ACS IMSI Pool Configuration Mode wherein the IMSI pool can be configured.

`-noconfirm`

Specifies that the command must execute without prompting for confirmation.

---

**Usage**

Use this command to create/configure/delete pools of International Mobile Subscriber Identifier (IMSI) numbers having group of single or range of IMSI numbers to use in access policy creation. The IMSI pool name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 IMSI pools can be created.

**Important:** IMSI pools in use in other ruledefs cannot be deleted.

---

**Example**

The following command creates an IMSI pool named `imsipool1`, and enters ACS IMSI Pool Configuration mode:

`imsi-pool  imsipool1`
ip max-fragments

This command limits the maximum number of IP fragments per fragment chain.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ip max-fragments max_fragments

default ip max-fragments

default ip max-fragments
Sets the maximum number of IP fragments limit to the default value.
Default: 45

max_fragments
Specifies the maximum number of IP fragments per fragment chain.
max_fragments must be an integer from 1 through 300.

Usage
Use this command to limit the maximum number of IP fragments.

Example
The following command limits the maximum number of IP fragments to 100.

ip max-fragments 100
**label**

This command defines a text string label to specific content ID for UDRs/EDRs/eG-CDRs in an Active Charging Service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
label content-id content_id text string
no label content-id content_id
```

**Usage**

Use this command to create a label string to attach to a specific content ID configured in the Charging Action Configuration Mode.
A maximum of 2048 labels can be configured within an Active Charging Service.

**Example**
The following command creates a label string `test_charge1` for content ID 1378:

```plaintext
label content-id 1378 text test_charge1
```
**nat allocation-failure**

Configures action to take when NAT IP/Port allocation fails.

**Important:** This command is only available in StarOS 8.3 and later releases.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```markdown
nat allocation-failure send-icmp-dest-unreachable
{ default | no } nat allocation-failure
```

- **default**
  Sets the default configuration.
  Default: Packets are dropped silently

- **no**
  Removes the previous NAT allocation failure configuration.
  When set, packets are dropped silently.

- **send-icmp-dest-unreachable**
  Specifies sending ICMP Destination Unreachable message when NAT IP/Port allocation fails.

**Usage**
Use this command to configure the action to take when NAT IP/port allocation fails—to send or not to send an “ICMP destination unreachable message” when a NAT IP/port cannot be assigned to a flow in data-path.

**Example**
The following command configures sending ICMP Destination Unreachable message when NAT IP/Port allocation fails:

```
nat allocation-failure send-icmp-dest-unreachable
```
**nat allocation-in-progress**

Configures action to take on packets when NAT IP/NPU allocation is in progress.

**Important:** This command is only available in StarOS 8.3 and later releases.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nat allocation-in-progress { buffer | drop }

default nat allocation-in-progress
```

- **default**
  Sets the default configuration.

- **buffer | drop**
  Specifies the action to take on packets when NAT IP/NPU allocation is in progress:
  - **buffer:** Specifies to buffer packets
  - **drop:** Specifies to drop packets
  Default: buffer

**Usage**
In On-demand NAT IP allocation (wherein NAT IP address is allocated to the subscriber when a packet is being sent), if no free NAT IP address is available, a NAT-IP Alloc Request is sent to the VPNMgr to get NAT-IP. During that time packets are dropped. This command enables buffering the packets received when IP Alloc Request is sent to VPNMgr.

**Example**
The following command specifies to buffer packets when NAT IP/NPU allocation is in progress:
```
nat allocation-in-progress buffer
```
nat tcp-2msl-timeout

This command configures TCP 2msl timeout configuration for NAT.

**Important:** This command is only available in StarOS 8.3 and later releases.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nat tcp-2msl-timeout timeout
default nat tcp-2msl-timeout
```

```
default
Sets the default configuration.
```

```
timeout
Specifies the TCP 2msl timeout in seconds, and must be an integer from 30 through 240. Default: 60 seconds
```

**Usage**

Use this command to configure the TCP 2msl timeout configuration for NAT.

**Example**

The following command configures the TCP 2msl timeout for NAT to 120 seconds:

```
nat tcp-2msl-timeout 120
```
p2p-detection protocol

This command configures the detection of specific peer-to-peer (P2P) protocols.

**Product**
P2P

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
[ no ] p2p-detection protocol [ actsync | aimini | all | applejuice | ares | battlefd | bittorrent | ddlink | directconnect | edonkey | fasttrack | feidian | filetopia | freenet | fring | gadugadu | gnutella | gtalk | halflife2 | hamachi | iax | imesh | iptv | irc | iskoot | jabber | manolito | msn | mute | nimbuzz | oovoo | openft | orb | oscar | paltalk | pando | pandora | popo | pplelive | ppstream | qq | qggame | qqlive | quake | rdp | secondlife | skinny | skype | slingbox | sopcast | soulseek | steam | tvants | tvuplayer | uusee | vpnx | vtun | warcft3 | winmx | winny | wofwarcraft | xbox | yahoo | zatattoo + ]
```

**all**
Configures the system to detect all of the P2P protocols. Specifying **all** is the same as configuring each protocol individually.

**actsync**
Configures the system to detect actsync protocols.

**aimini**
Configures the system to detect aimini protocols.

**applejuice**
Configures the system to detect applejuice protocols.

**ares**
Configures the system to detect ares protocols.

**battlefd**
Configures the system to detect battlefd protocols.

**bittorrent**
Configures the system to detect bittorrent protocols.

**ddlink**
Configures the system to detect ddlink protocols.

**directconnect**
Configures the system to detect directconnect protocols.

**edonkey**
Configures the system to detect edonkey protocols.
### Active Charging Service Configuration Mode Commands

#### Fast Track
Configures the system to detect fasttrack protocols.

#### Feidian
Configures the system to detect feidian protocols.

#### Filetopia
Configures the system to detect filetopia protocols.

#### Freenet
Configures the system to detect freent protocols.

#### Fring
Configures the system to detect fring protocols.

#### Gadugadu
Configures the system to detect gadugadu protocols.

#### Gnutella
Configures the system to detect gnutella protocols.

#### Gtalk
Configures the system to detect gtalk protocols.

#### Halflife2
Configures the system to detect halflife2 protocols.

#### Hamachivpn
Configures the system to detect hamachivpn protocols.

#### Iax
Configures the system to detect iax protocols.

#### Imesh
Configures the system to detect imesh protocols.

#### Iptv
Configures the system to detect iptv protocols.

#### Irc
Configures the system to detect irc protocols.

#### Iskoot
Configures the system to detect iskoot protocols.

#### Jabber
Configures the system to detect jabber protocols.
Active Charging Service Configuration Mode Commands

- **manolito**
  Configures the system to detect manolito protocols.

- **msn**
  Configures the system to detect msn protocols.

- **mute**
  Configures the system to detect mute protocols.

- **nimbus**
  Configures the system to detect nimbus protocols.

- **oovoo**
  Configures the system to detect oovoo protocols.

- **openft**
  Configures the system to detect openft protocols.

- **orb**
  Configures the system to detect orb protocols.

- **oscar**
  Configures the system to detect oscar protocols.

- **paltalk**
  Configures the system to detect paltalk protocols.

- **pando**
  Configures the system to detect pando protocols.

- **pandora**
  Configures the system to detect pandora protocols.

- **popo**
  Configures the system to detect popo protocols.

- **pplive**
  Configures the system to detect pplive protocols.

- **ppstream**
  Configures the system to detect ppstream protocols.

- **qq**
  Configures the system to detect qq protocols.

- **qggame**
  Configures the system to detect qggame protocols.

- **qqlive**
  Configures the system to detect qqlive protocols.
Active Charging Service Configuration Mode Commands

- **p2p**

  Configures the system to detect quake protocols.

- **rdp**

  Configures the system to detect rdp protocols.

- **secondlife**

  Configures the system to detect secondlife protocols.

- **skiny**

  Configures the system to detect skinny protocols.

- **skype**

  Configures the system to detect skype protocols.

- **slingbox**

  Configures the system to detect slingbox protocols.

- **sopcast**

  Configures the system to detect sopcast protocols.

- **soulseek**

  Configures the system to detect soulseek protocols.

- **steam**

  Configures the system to detect steam protocols.

- **tvants**

  Configures the system to detect tvants protocols.

- **tvuplayer**

  Configures the system to detect tvuplayer protocols.

- **uusee**

  Configures the system to detect uusee protocols.

- **vpn)**

  Configures the system to detect vpx protocols.

- **vtun**

  Configures the system to detect vtun protocols.

- **warcft3**

  Configures the system to detect warcf3 protocols.

- **winmx**

  Configures the system to detect winmx protocols.
Active Charging Service Configuration Mode Commands

p2p-detection protocol

---

**winny**
Configures the system to detect winny protocols.

---

**wofwarcraft**
Configures the system to detect wofwarcraft protocols.

---

**xbox**
Configures the system to detect xbox protocols.

---

**yahoo**
Configures the system to detect yahoo protocols.

---

**zatoo**
Configures the system to detect zatoo protocols.

---

+ More than one of the above keywords can be entered within a single command.

---

**Usage**
Use this command to configure the detection of specific P2P protocols. Multiple commands can be specified in the command.

---

**Example**
The following command enables detection of all P2P protocols:

```
p2p-detection protocol all
```
p2p-dynamic-rules

This command enables/disables the P2P Dynamic Signature Updates feature, and loads the P2P signature file from the default or specified location into memory, optionally signatures for specific protocol(s) can be specified to be loaded.

**Important:** This release supports dynamic updates of signatures (detection logic) only for the following protocols: Bittorrent, DirectConnect, eDonkey, Gnutella, Skype, and Yahoo.

**Product**: P2P

**Privilege**: Security Administrator, Administrator

**Syntax**

```
p2p-dynamic-rules { file location [ force ] | protocol [ all | bittorrent | directconnect | edonkey | gnutella | skype | yahoo + ] }
```

```
default p2p-dynamic-rules file
```

```
no p2p-dynamic-rules { file | protocol [ all | bittorrent | directconnect | edonkey | gnutella | skype | yahoo + ] }
```

```
default
```

Enables the P2P Dynamic Signature Updates feature, and if available, loads the P2P signature file from the default location: /usr/lib/p2p-rules.xml.

```
no
```

Disables the P2P Dynamic Signature Updates feature, also any/specified signature(s) already loaded in the memory is unloaded.

If there are any active sessions using the file, it changes the file status to inactive. And, when the sessions are cleared, the file is removed from the memory.

```
file location
```

Specifies that the P2P signature file at the specified location (other than the default location) be loaded into memory and applied.

`location` specifies the file’s location, and must be one of the following:

[file://] /flash | /pcmcia1 | /hd-raid]/[directory]/<filename>

```
force
```

Specifies to force load the specified file into memory and apply it, even if it is obsolete.

By default, when a signature file is loaded from a specified location `file location`, while loading, it is compared with the file at the default location. The newer file of the two files is loaded into memory. To override this behavior, use the `force` keyword.
protocol [ all | bittorrent | directconnect | edonkey | gnutella | skype | yahoo + ]

Specifies the protocols for which signatures must be enabled for processing. 
+ indicates that more than one of the keywords can be specified in the same command. Not applicable if the all option is selected first.

Usage
Use this command to enable/disable the P2P Dynamic Signature Updates feature, and load the P2P signature file from the default or specified location. Optionally the specific protocol(s) for which the signatures must be loaded can be specified.

Example
The following command enables the P2P Dynamic Signature Updates feature, and loads the signature file present in the default location:

default p2p-dynamic-rules file
packet-filter

This command enables creating/configuring/deleting an Active Charging Service packet filter.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
packet-filter filter_name [ -noconfirm ]
```

```
o no packet-filter filter_name
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Removes the specified packet filter, if configured previously.

<table>
<thead>
<tr>
<th>filter_name</th>
</tr>
</thead>
</table>
| filter_name must be the name of the packet filter, and must be a string of 1 through 63 characters in length. If the named packet filter does not exist, it is created, and the CLI mode changes to the Packet Filter Configuration Mode wherein the packet filter can be configured. If the named packet filter already exists, the CLI mode changes to the Packet Filter Configuration Mode wherein the packet filter can be configured.

<table>
<thead>
<tr>
<th>-noconfirm</th>
</tr>
</thead>
</table>
| Specifies that the command must execute without prompting for confirmation.

Usage
Use this command to create/configure/delete an ACS packet filter.

Example
The following command creates a packet filter named filter3, and enters the Packet Filter Configuration Mode:

```
packet-filter filter3
```
passive-mode

This command configures the Active Charging Service to operate in passive mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ default | no ] passive-mode

  no
  Specifies to disable passive mode.

  default
  Sets the default setting.
  Default: Disabled

Usage
Use this command to put the Active Charging Service in/out of passive mode operation. Configures whether the Active Charging Service passively monitors copies of packets.

Example
The following command puts the Active Charging Service into passive mode operation:

  passive-mode
**policy-control burst-size**

This command configures the burst size for bandwidth limiting per dynamic-rule or per bearer.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
policy-control burst-size { auto-readjust [ duration duration ] | bytes bytes }
{ default | no } policy-control burst-size
```

- **default | no**
  Sets the default configuration.
  Default: 65535 bytes

- **auto-readjust**
  Configures the burst size equal to <seconds> of traffic.
  Default: 10 seconds

- **duration duration**
  Specifies the seconds of traffic configured for burst size.
  `duration` must be an integer from 1 through 20.

- **bytes bytes**
  Configures the burst size in bytes.
  `bytes` must be an integer from 1 through 4000000000.

**Usage**
Use this command to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

**Example**
The following command configures the burst size for bandwidth limiting per dynamic-rule or per bearer equal to 10 seconds of traffic:

```
policy-control burst-size auto-readjust
```
policy-control charging-rule-base-name

This command configures interpretation of Charging-Rule-Base-Name AVP from PCRF either as active-charging rulebase or active charging group-of-ruledefs.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
policy-control charging-rule-base-name { active-charging-group-of-ruledefs | active-charging-rulebase [ ignore-when-removed ] }

default policy-control charging-rule-base-name
```

- `default`
  Sets the default configuration.
  Default: `active-charging-group-of-ruledefs`

- `active-charging-group-of-ruledefs`
  Specifies interpreting Charging-Rule-Base-Name as active-charging group-of-ruledefs.

- `active-charging-rulebase [ ignore-when-removed ]`
  Specifies interpreting Charging-Rule-Base-Name as active-charging rulebase.
  When Charging-Rule-Base-Name AVP is interpreted as active-charging rulebase, if PCRF requests the removal of a Charging-Rule-Base-Name, which is the same as the rulebase used for that PDP context, the PDP context is terminated. This is because after removal of the rulebase, the PDP context will have no rulebase. This is the default behavior.
  When the `ignore-when-removed` option is configured, PCRF request for removal of Charging-Rule-Base-Name is ignored and no action is taken.
  For each call, this interpretation is decided at call setup, and will not be changed during the life of that call. Change will only apply to new calls coming up after the change.

Usage

Use this command to configure interpretation of Charging-Rule-Base-Name AVP from PCRF either as active charging group-of-ruledefs or as active-charging rulebase.

Example

The following command configures interpreting of Charging-Rule-Base-Name AVP as active-charging rulebase:

```
policy-control charging-rule-base-name active-charging-rulebase
```
**port-map**

This command enables creating/configuring/deleting a port map.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
port-map port_map [ -noconfirm ]
no port-map port_map
```

- **no**
  Removes the specified port map.

- **port_map**
  Specifies the port map name.
  `port_map` must be a string of 1 through 63 characters in length, and can contain punctuation characters.
  If the named port map does not exist, it is created, and the CLI mode changes to the ACS Port Map Configuration Mode wherein the port map can be configured.
  If the named port map already exists, the CLI mode changes to the ACS Port Map Configuration Mode wherein the port map can be configured.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a port map.
The port map name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 port maps can be created.

**Important:** Port maps in use in other ruledefs cannot be deleted.

**Example**
The following command creates a port map named `portmap1`, and enters ACS Port Map Configuration mode:

```
port-map portmap1
```
redirect user-agent

This command specifies the user agent for conditional redirection of traffic flows.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] redirect user-agent user_agent_name

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified user agent.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>user_agent_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the user agent to be used for redirecting traffic flow.</td>
</tr>
<tr>
<td>user_agent_name must be an alpha and/or numeric string of 1 through 32 characters in length.</td>
</tr>
<tr>
<td>A maximum of 16 user-agents can be configured in an Active Charging Service.</td>
</tr>
</tbody>
</table>

Usage

Use this command to redirect the traffic flow with conditions based on configured user-agent name. This user agent is used with flow action command in the Charging Action Configuration Mode.

Example

Following command specifies the redirect user agent user_rule1 for conditional redirection of traffic flow.

redirect user-agent user_rule1
rulebase

This command enables creating/configuring/deleting an ACS rulebase.

**Important:** A maximum of 512 rulebases can be configured in an Active Charging Service.

<table>
<thead>
<tr>
<th>Product</th>
<th>ECS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax**

```
rulebase rulebase_name [ -noconfirm ]
```

```
no rulebase rulebase_name
```

- **no**
  Removes the specified rulebase from the current Active Charging Service.

- **rulebase_name**
  - `rulebase_name` must be an alpha and/or numeric string of 1 through 63 characters in length, and can contain punctuation characters.
  - If the named rulebase does not exist, it is created, and the CLI mode changes to the ACS Rulebase Configuration Mode wherein the rulebase can be configured.
  - If the named rulebase already exists, the CLI mode changes to the ACS Rulebase Configuration Mode wherein the rulebase can be configured.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matched flow. The `rulebase_name` must be unique for a given Active Charging Service.

The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

**Example**

The following command creates a rulebase named `test1`, and enters the ACS Rulebase Configuration mode:

```
rulebase test1
```
ruledef

This command enables creating/configuring/deleting a rule definition in an Active Charging Service.

**Important:** A maximum of 2048 ruledefs can be configured in an Active Charging Service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ruledef ruledef_name [ -noconfirm ]

no ruledef ruledef_name
```

- **no**
  Removes the specified ruledef from the current Active Charging Service.

- **ruledef_name**
  ruledef_name must be an alpha and/or numeric string of 1 through 63 characters in length, and can contain punctuation characters.
  ruledef_name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.
  If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
  If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete an ACS ruledef.
A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the Active Charging Service.

**Example**

The following command creates a rule definition named test1, and enters ACS Ruledef Configuration mode

```
ruledef test1
```
system-limit

This command configures the system-wide Layer 4 flow limit.

**Important:** This command is customer specific. For more information, please contact your local sales or service representative.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
system-limit 14-flows limit
{ default | no } system-limit 14-flows
```

**Default**
Sets the default configuration.
Default: `no system-limit 14-flows`

**no**
Disables the limit checking.

**limit**
Specifies the Layer 4 flows limit, and must be an integer from 1 through 2147483647.

**Usage**

Use this command to configure the system-wide limit for Layer 4 flows.
The System-wide L4 Flow Limiting feature provides the capability to limit the number of TCP and UDP flow over the system. This limiting can be applied to all subscribers attaching to the system and to all APNs. This feature is compatible with the existing per-subscriber limiting (configured using the flow limit-for-flow-type charging action). Both limiting can be active in the same time.
System-wide flow limiting is implemented by comparing the “Effective Flows” periodically (~ every 10 seconds) against the configurable “System-wide Flow Limit”. Where “Effective Flows” is the number of active data sessions, each identified by 5 tuple key. If the “Effective Flows” exceeds the “System-wide Flow Limit”, the Resource Manager indicates it to the ECS service. Once ECS is aware of the “System-wide Flow Limit” being reached, no more data sessions are setup. The packets are discarded. While processing a successive flow-usage update from ECS service a change in behavior is indicated to ECS service to start accepting data sessions. As this relies on periodic reporting there is an inherent delay in the detection of “exceeding/returning once exceeded” to the flow limit.

**Example**
The following command sets the system limit for L4 flows to 100:

```
```
system-limit 14-flows 100
**timedef**

This command enables creating/configuring/deleting a Time Definition (timedef).

**Important:** This command is only available in StarOS 8.1 and StarOS 9.0 and later releases.

**Important:** A maximum of 10 timedefs can be configured in an Active Charging Service.

**Product**

ECS

**Privilege**

Security Administrator, Administrator

**Syntax**

```
timedef timedef_name [ -noconfirm ]
no timedef timedef_name
```

**no**

Deletes the specified timedef.

**timedef_name**

*timedef_name* specifies name of the timedef, and must be an alpha and/or numeric string of 1 through 63 characters in length.

If the named timedef does not exist, it is created, and the CLI mode changes to the Timedef Configuration Mode wherein timeslots for the timedef can be configured.

If the named timedef already exists, the CLI mode changes to the Timedef Configuration Mode wherein timeslots for the timedef can be configured.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete ACS timedefs for the Time-of-Day Activation/Deactivation of Rules feature. Timedefs enable activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only when they are active.

**Example**

The following command creates a timedef named *test1*, and enters the ACS Timedef Configuration mode:

```
timedef test1
```
udr-format

This command creates/configures/deletes an UDR format specification.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
udr-format name [ -noconfirm ]
no udr-format name
```

no
Removes the specified UDR format in the current Active Charging Service.

name
Specifies UDR format name, and must be an alpha and/or numeric string of 1 through 63 characters in length.
If the named UDR format does not exist, it is created, and the CLI mode changes to the UDR Format Configuration Mode wherein the UDR format can be configured.
If the named UDR format already exists, the CLI mode changes to the UDR Format Configuration Mode wherein the UDR format can be configured.
Up to 256 UDR and/or EDR formats can be configured in a system across all Active Charging Services.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage
Use this command to create/configure/delete an UDR format for a specific Active Charging Service.

Example
The following command creates an UDR format named udr_format1:
```
udr-format udr_format1
```
url-blacklisting match-method

This command sets the match method to look up URLs in the URL Blacklisting database.

Product
CF

Privilege
Security Administrator, Administrator

Syntax
url-blacklisting match-method { exact | generic }

default url-blacklisting match-method

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: exact</td>
</tr>
<tr>
<td>Sets the default match method.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>exact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the exact-match method, wherein URL Blacklisting is performed only on exact match with URLs present in the URL Blacklisting database.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>generic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the generic-match method, wherein URL Blacklisting is performed on generic match with URLs present in the URL Blacklisting database.</td>
</tr>
</tbody>
</table>

Usage
Use this command to set the match method to look up URLs in the URL Blacklisting database.

Example
The following command sets the exact-match method to look up URLs in the URL Blacklisting database:

url-blacklisting match-method exact
xheader-format

This command enables creating/configuring/deleting an extension-header (x-header) format specification for the current Active Charging Service.

⚠️ Important: This is a customer-specific command. For more information, please contact your local sales representative.

<table>
<thead>
<tr>
<th>Product</th>
<th>ECS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

### Syntax

```
xheader-format xheader_format_name [ -noconfirm ]
```

```
no xheader-format xheader_format_name
```

- `no` Removes the specified x-header format for the current Active Charging Service.

- `xheader_format_name` Specifies the x-header format name. `xheader_format_name` must be an alpha and/or numeric string of 1 through 63 characters in length. If the named x-header format does not exist, it is created, and the CLI mode changes to the x-header Format Configuration Mode wherein the x-header format can be configured. If the named x-header format already exists, the CLI mode changes to the x-header Format Configuration Mode wherein the x-header format can be configured.

- `-noconfirm` Specifies that the command must execute without prompting for confirmation.

### Usage

Use this command to create/configure/delete an x-header format specification for a specific Active Charging Service. An x-header may be specified in a charging action to be inserted into HTTP GET and POST request packets. See `xheader-insert` CLI command in the Charging Action Configuration Mode Commands, and x-header Format Configuration Mode Commands chapter.

### Example

The following command creates an x-header format named test, and enters the x-header Format Configuration Mode:

```
xheader-format test
```
Chapter 12
ALCAP Configuration Mode Commands

The ALCAP Service Configuration Mode is used to create, provide, and manage the Access Link Control Application Part (ALCAP) on HNB-GW to support IuCS-over-ATM connectivity to HNB subscriber in a 3G UMTS networks towards CS core network.
aal2-node

This command creates/configures AAL2 node configuration to defined AAL2 node properties for IuCS-over-ATM function.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
  aal2-node aal2_node_name [-noconfirm]
  [no] aal2-node aal2_node_name
```

no

Removes the configured AAL2 node from ALCAP service configuration.

```
  aal2_node_name
```

Identifies the name of the AAL2 node name to configure the AAL2 node parameters. The `aal2_node_name` must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to create/configure the AAL2 node configuration and switch to AAL2 Node Configuration mode.

Entering this command results in the following prompt:

```
  [context_name]hostname(config-aal2-node-aal2_node_name)#
```

A maximum of TBD AAL2 node can be configured in one ALCAP service.

Important: The AAL2 Node configured here will be used to bind with ATM port in PVC Configuration sub-mode of ATM Configuration mode for IuCS-over-ATM functionality.

Important: For more information on AAL2 node configuration, refer AAL2 Node Configuration Mode Commands.

Example

Following command creates AAL2 node configuration mode named `aal2_1` within the specific ALCAP service for IuCS-over-ATM support towards CS core networks and switch the user to AAL2 Node Configuration Mode named `aal2_1`:

```
  aal2-node aal2_node_name -noconfirm
```
### aal2-route

This command defines a route for each ATM Endpoint Service Address (AESA) with which it can have transport layer communication. This route actually maps an AESA to one or more AAL2 paths which will be used to setup an end to end communication path.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
aal2-route end-point [AESA_address | default] aal2-node aal2_node_name

[no] aal2-route end-point [AESA_address | default] [aal2-node aal2_node_name]
```

**no**

Removes defined AAL2 route from ALCAP service configuration.

| end-point [AESA_address | default] |
|-------------------------------------|

Specifies the AESA address in an ATM (or AAL2) network to map with adjacent AAL2 node. The AESA is based on the generic network service access point (NSAP) format. The ATM connection from HNB-GW terminates at this point.

The AESA_address must be an alpha/numeric string from 1 through 63 characters.

The default keyword is used to configure a default AAL2 route which will match any AESA received from MSC and for which AESA specific route is not configured. When a connection is established an AESA specific route will have higher priority than default route.

**Usage**

Use this command to create a mapping between ATM endpoint and adjacent node for AAL2 connection routing purposes.

It defines a route for each ATM Endpoint Service Address (AESA) with which it can have transport layer communication. This route actually maps an AESA to one or more AAL2 paths which will be used to setup an end to end communication path.

The default keyword can be used to configure a default aal2-route which will match any AESA received from MSC and for which AESA specific route is not configured. When a connection is established an AESA specific route will have higher priority than default route.

**Important:** The default route shall not be used when AESA specific route exists.

If an HNB-GW configured with a route for MGW1 which consists of AAL2_path_A and AAL2_path_B for AAL2 switch-A and AAL2 switch-B switch respectively then similarly AAL2 switch-A and AAL2 switch-B need to be configured with routes for MGW1.

A maximum of TBD AAL2 routes can be configured in one ALCAP service.

**Example**

| OL-22948-01 | 393 | Cisco ASR 5000 Series Command Line Interface Reference |
Following command create a mapping between ATM endpoint \textit{MGW1} and AAL2 node \textit{aal2_1} for AAL2 connection routing purposes:

\texttt{aal2-route end-point [MGW1 aal2-node aal2_1}
associate

This command associates a previously configured SS7 routing domain with this ALCAP service on HNB-GW node which will be used to define the SS7 routing domain in 3G UMTS networks.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
associate ss7-routing-domain ss7_rd_id
```

```
no associate ss7-routing-domain
```

**no**

Removes the associated SS7 routing domain id from this ALCAP service configuration.

**ss7_rd_id**

Identifies the SS7 routing domain index configured in Global configuration mode to associate with ALCAP service for IuCS-over-ATM support.

The `ss7_rd_id` must be an integer from 1 through 12.

**Important:** For SS7 routing domain configuration, refer *SS7 Routing Domain Configuration Commands Mode* chapter.

**Usage**

Use this command to associate a preconfigured SS7 routing domain index to provide IuCS-over-ATM support towards CS core network for HNB subscriber.

A maximum of *TBD* SS7 routing domains can be configured in one ALCAP service.

**Example**

Following command associates a predefined SS7 routing domain id 3 with ALCAP service to define routing domain for IuCS-over-ATM suppport towards CS core networks:

```
associate ss7-routing-domain 3
```
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the previous mode.
maximum reset-retransmission

This command sets the maximum number of retries allowed for transmission of RESET message to reset the AAL2 path.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax
maximum reset-retransmissions retries

default maximum reset-retransmissions

Examples

Sets the number of RESET message retries to default value of 1.

retires

Sets the maximum number of retries allowed for transmission of RESET message to reset the AAL2 path by ALCAP service.

retires must be an integer value from 0 through 4. When 0 is used retransmission will be disabled. Default: 1

Usage
Use this command to sets the maximum number of retries allowed for transmission of RESET message by ALCAP service to reset the AAL2 path when Timer_RES expires. Once the maximum number of RESET retries have been performed the ALCAP service shall stop the RESET procedure for the affected path and path will become available for connections.

Example
The following command configures ALCAP service to send maximum number of 2 RESET messages after expiry of RESET timer for AAL2 path RESET procedure:

```
maximum reset-retransmissions 2
```
self-point-code

This command specifies the SS7 point code address for ALCAP service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

self-point-code point_code

no self-point-code

---

no

Deletes the configured self point code for this ALCAP service.

---

point_code

Defines the point code to assign to this ALCAP service.

Value entered must adhere to the point code variant selected when the ALCAP service instance was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- A string of 1 to 11 combined digits and period.

---

Usage

Use this command to assign the self point code to use for this ALCAP service.

---

Example

The following command sets an ITU-based point code for this ALCAP service:

self-pointcode 4.121.5

The following command removes the configured self-point code:

no self-pointcode
timeout alcap

This command configures the timeout duration for various ALCAP procedure timers in ALCAP service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

timeout alcap \{blo blo_timer_value | erq erq_timer_value | mod mod_timer_value | rel rel_timer_value | res res_timer_value | ubl ubl_timer_value\}

default timeout alcap \{blo | erq | mod | rel | res | ubl\}

default

Sets the timer values to default duration for specific ALCAP procedure in an ALCAP service.

blo blo_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Path Block procedure. When a request to block a particular AAL2 path is received by ALCAP service, the ALCAP service sends ALCAP-BLOCK-REQUEST message to AAL2 node/peer ALCAP Manage and starts Timer_BLO timer. The timer waits for specified timeout duration blo_timer_value for ALCAP-BLOCK-CONFIRM message before reporting error in procedure. If AAL2 Node responds with ALCAP-BLOCK-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.

Default: 5

erq erq_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Establish Request procedure. When a request to establish a connection through ALCAP-ESTABLISH-REQUEST message is sent to AAL2 node the system starts the Timer_ERQ timer. The timer waits for specified timeout duration erq_timer_value for ALCAP-ESTABLISH-CONFIRM message before reporting error in procedure and system requests ALCAP Manager to free the AAL2-channel used for connection and also indicates to start the RESET procedure for this channel. If AAL2 Node responds with ALCAP-ESTABLISH-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.

Default: 5

mod mod_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Modify Request procedure. When a request to modify a connection or channel through ALCAP-MODIFY-REQUEST message is sent to AAL2 node the system starts the Timer_MOD timer. The timer waits for specified timeout duration mod_timer_value for ALCAP-MODIFY-CONFIRM message before reporting error in procedure and system requests ALCAP Manager to initiates the
RESET or any other appropriate procedure for this channel and HNB-GW shall release the RUA connection towards HNB and SCCP connection towards CN.
If AAL2 Node responds with ALCAP-MODIFY-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure. 

mod_timer_value must be an integer value from 5 through 30.
Default: 5

rel rel_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Release Request procedure. When a request to release a connection or channel through ALCAP-RELEASE-REQUEST message is sent to AAL2 node the system starts the Timer_REL timer and sends RAB-ASST-REQ to HNB. The timer waits for specified timeout duration rel_timer_value for ALCAP-RELEASE-CONFIRM message before reporting error in procedure and system requests ALCAP Manager to release the AAL2 channel. System also indicates to start RESET procedure for this channel.
If AAL2 Node responds with ALCAP-RELEASE-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
rel_timer_value must be an integer value from 2 through 60.
Default: 2

res res_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Reset Request procedure. When a request to reset a connection or channel through ALCAP-RESET-REQUEST message is sent to AAL2 node the system starts the Timer_RES timer. The timer waits for specified timeout duration res_timer_value for ALCAP-RESET-CONFIRM message before retrying the RESET procedure. The system will retry the RESET procedure for configured number of times and on completion of retry limit the stops the RESET procedure for the affected path and path will become available for connections.
If AAL2 Node responds with ALCAP-RESET-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
res_timer_value must be an integer value from 2 through 60.
Default: 2

ubl ubl_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Path UnBlock procedure. When a request to unblock a particular AAL2 path is received by ALCAP service, the ALCAP service sends ALCAP-UNBLOCK-REQUEST message to AAL2 node/peer ALCAP Manager and start Timer_BLO timer. The timer waits for specified timeout duration ubl_timer_value for ALCAP-UNBLOCK-CONFIRM message before reporting error in procedure. If AAL2 node/peer ALCAP Manager responds with ALCAP-BLOCK-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
ubl_timer_value must be an integer value from 2 through 60.
Default: 2

Usage

Use this command to configure the timeout duration for various ALCAP procedures in ALCAP service.

Example
The following command sets the timeout duration of 10 seconds for ALCAP-MODIFY-REQUEST procedure:

```
timeout alcap mod 10
```
timeout stc

This command configures the timeout duration for STC long (T30) and and STC short (T29) timers used in congestion indication procedure at Signaling Transport Converter (STC) layer in ALCAP service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

timeout stc {long long_timer_value | short short_timer_value}

timeout stc {long | short}

default

Sets the timer values to default duration for specific STC procedure in an ALCAP service.

long long_timer_value

Specifies the duration in milliseconds for STC long timer. This timer is used by the congestion indication procedure. Receipt of a repeated congestion indication from MTP3B before the expiry of this timer is interpreted as the congestion situation. On the other hand, if no congestion indication is received from MTP3B before expiry of this timer, the congestion situation is considered to have improved.

long_timer_value must be an integer value from 5000 through 10000.

Default: 5000

short short_timer_value

Specifies the duration in milliseconds for STC short timer. This timer is used by the congestion indication procedure. The role of this timer is to avoid overreacting if multiple congestion indications are received from MTP3B in quick succession.

short_timer_value must be an integer value from 300 through 600.

Default: 300

Usage

Use this command to configure the long (T30) and short (T29) timer for congestion indication procedure in ALCAP service.

When the first congestion indication is received by, the traffic load into the affected destination point code is reduced and the same time two timers STC short timer (T29) and STC long timer (T30) are started. During STC short timer all received congestion indications for the same destination point code are ignored in order not to reduce traffic too rapidly. Reception of a congestion indication after the expiry of STC short timer, but still during STC long timer, will decrease the traffic load by one more step and restart both the timers again. If STC long timer expires (i.e. no congestion indications having been received during the STC long timer period), traffic will be increased by one step and STC long timer will be restarted unless full traffic load has been resumed.

Example
The following command sets the timeout duration of 5000 milliseconds for STC long timer:

```
default timeout stc long
```

The following command sets the timeout duration of 300 milliseconds for STC short timer:

```
default timeout stc short
```
Chapter 13
APN Configuration Mode Commands

The Access Point Name (APN) Configuration Mode is used to create and configure APN profiles within the current system context of a UMTS/LTE service.

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

This command configures a AAA server group for the APN for AAA functionality.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

[ no ] aaa group group_name

default aaa group

no
Disables the specified AAA group for the specific APN.

default
Sets / restores default AAA group specified at the context level or in APN template.

group_name
The AAA group to configure for the APN.
group_name must be a string of 1 through 63 characters in length.

Usage
Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for APNs in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).

Example
The following command applies the AAA server group star1 to an APN within the specific context:

    aaa group star1

The following command disables the AAA group for the specific APN:

    no aaa group group_name
**access-link**

Configures IP fragmentation processing over the Access-link (PPP, GTP etc).

**Product**

GGSN, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }
```

- **df-ignore**
  
  Default: Disabled
  Ignore the DF bit setting. Fragment and forward the packet over the access link.

- **df-fragment-and-icmp-notify**
  
  Default: Disabled
  Partially ignore the DF bit. Fragment and forward the packet, but also return an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to 1 ICMP error packet per second per session.

- **normal**
  
  Default: Enabled
  Normal processing. Drop the packet and send an ICMP unreachable message to the source of packet. This is the default behavior.

**Usage**

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.

Note that regardless of whether or not fragmentation is performed because of one of the above reasons, fragmentation may also occur for other reasons.

Payloads are encapsulated within IP/UDP/GTP before being sent to the SGSN. If that encapsulation causes the packet to exceed 1500 bytes, the inner IP payload is fragmented (even if it's not considered too-large by the above tests) into two payloads (if the DF bit is not set). If the DF bit is set (and access-link ip-fragmentation normal is configured), the system performs IP fragmentation of the entire packet (i.e., IP fragmentation in the outer IP header) rather than fragmenting the inner IP payload. Either way, the result is two packets, but in one case the MS would have to perform IP reassembly while in the other case the SGSN would have to perform reassembly.

**Example**

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command:
access-link ip-fragmentation df-ignore
accounting-mode

This command configures the protocol to be used for PDP context accounting by this APN.

Product
GGSN, ECS, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
accounting-mode { gtpp | none | radius-diameter [ no-interims ] [ no-early-pdu-s ] }
default accounting-mode
```

default
Restores the command to its default setting.

```
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gtpp</td>
<td>Configures the APN to use GPRS Tunneling Protocol Prime for accounting purposes. If used, accounting will begin as soon as the PDP context is established. This is the default setting. Default: Enabled</td>
</tr>
<tr>
<td>none</td>
<td>Disables accounting for PDP contexts using this APN. When accounting mode is set to none, it indicates to the GTP stack at session manager to not generate the regular GTPP accounting triggers. Default: Disabled.</td>
</tr>
<tr>
<td>radius-diameter</td>
<td>Configures the APN to use RADIUS/Diameter protocol for accounting purposes. Default: Disabled</td>
</tr>
</tbody>
</table>

**Important:** The system’s GTPP parameters must be configured prior to using this protocol for accounting. Refer to the gtpp commands in the Context Configuration Mode Commands chapter of this reference.

```
no-early-pdus
Configures the GGSN to discard user traffic once the buffer is full until the RADIUS server has returned a response to the GGSN's accounting START request per 3GPP standards.
```

**Important:** The system’s RADIUS/Diameter accounting parameters must be configured prior to using either of the protocols for accounting. Refer to the radius/diameter commands in the Context Configuration Mode Commands and the AAA Server Group Configuration Mode Commands chapters of this reference.
no-interims

Disables the generation of RADIUS interims per APN. If no-interims is specified, then it won't send any RADIUS INTERIM-UPDATEs for this APN, regardless of what is configured in the context that is used for RADIUS accounting.

Usage

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile. When the GTPPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPPP functionality are typically configured within the system’s source context. As specified by the standards, a CDR is not generated when a session starts - CDRs are generated according to the interim triggers (configured using the cc command in the GGSN service configuration mode) and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.

GTPP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTPPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

If the radius-diameter option is used, either the RADIUS or the Diameter protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.

If the RADIUS protocol is used, accounting messages can be sent over a AAA interface or the Gi to the RADIUS server. The AAA or Gi interface(s) and RADIUS functionality are typically configured with the system’s destination context along with the APN. RADIUS accounting begins immediately after an IP address is allocated for the MS. Interim accounting can be configured using the radius accounting interim interval. The radius accounting interim interval command sends INTERIM-UPDATE messages at specific intervals.

Keywords to this command can be used in combination to each other, depending on configuration requirements.

Important: If the accounting type in the APN is set to ‘none’ then G-CDRs will not be generated. If accounting type is left as default ‘GTPP’ and ‘billing-records’ are configured in Rulebase configuration mode in ECS, then both G-CDRs and eG-CDRs would be generated.

Example

The following command configures the APN to use the RADIUS/Diameter protocol for accounting:

```
accounting-mode radius-diameter
```

```
accounting-mode radius-diameter no-interims no-early-pdus
```

```
accounting-mode radius-diameter no-early-pdus no-interims
```
active-charging bandwidth-policy

This command configures the bandwidth policy to be used for subscribers who use this APN.

Product
GGSN, ECS

Privilege
Security Administrator, Administrator

Syntax

active-charging bandwidth-policy bandwidth_policy
{ default | no } active-charging bandwidth-policy

**default**
Specifies that the default bandwidth policy configured in the rulebase be used for subscribers who use this APN.

**no**
Disables bandwidth control for the APN.

**bandwidth_policy**
Specifies the bandwidth policy name.
*bandwidth_policy* must be an alpha and/or numeric string from 1 through 63 characters in length.

Usage
Use this command to configure bandwidth policy to be used for subscribers who use this APN.

Example
The following command configures a bandwidth policy named *standard* for the APN:

```
active-charging bandwidth-policy standard
```
active-charging rulebase

This command specifies the name of the ACS rulebase to be used for subscribers who use this APN.

Product
GGSN, ECS, P-GW

Privilege
Security Administrator, Administrator

Syntax

active-charging rulebase rulebase_name

no active-charging rulebase

no
Removes the rulebase previously specified for this APN.

rulebase_name
Specifies the ACS rulebase name.
rulebase_name must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage
Use this command to specify the name of the ACS rulebase to be used for subscribers who use the APN.

Example
The following command specifies the ACS rulebase rule1 for the APN:

active-charging rulebase rule1
apn-ambr

Configures the Aggregated Maximum Bit Rate (AMBR) for all PDNs using this APN.

Product
P-GW

Privilege
Administrator

Syntax

```bash
apn-ambr rate-limit direction { downlink | uplink } [ burst-size { auto-readjust duration seconds | bytes } | violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ]
[ default | no ] apn-ambr rate-limit direction { downlink | uplink }
```

default
Returns the selected command to it’s default setting of no APN-AMBR.

no
Disables the selected command.

direction { downlink | uplink }
Specifies that the rate limit is to be applied to either the downlink traffic or the uplink traffic.

downlink: Applies the AMBR parameters to the downlink direction.

uplink: Applies the AMBR parameters to the uplink direction.

burst-size { auto-readjust duration seconds | bytes }
This parameter is used by policing and shaping algorithms to permit short bursts of traffic in order to not exceed the allowed data rates. It is the maximum size of the token bucket.

auto-readjust duration seconds: A duration, in seconds, used in this burst size calculation:

\[
\text{burst size} = \text{peak data rate}/8 \times \text{auto-readjust duration}
\]

seconds must be an integer value from 1 to 30. Default is 1 second

bytes: Specifies the burst size in bytes allowed by this APN for the associated PDNs. bytes must be an integer value from 1 to 4294967295 (1 byte to 4 GB).

violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit }
The action that the P-GW will take when the data rate of the bearer context exceeds the AMBR.

drop: Violating packets are dropped.

lower-ip-precedence: The DSCP value is set to zero (“best effort”) for the violating packets.

shape { transmit-when-buffer-full }: Place all violating packets into a buffer and, optionally, packets are transmitted when the buffer is full.

transmit: Violating packets are transmitted. This is the default setting.

Usage
Use this command to enforce the AMBR for the APN on bearers that do not have a Guaranteed Bit Rate (GBR).

Example
The following command sets the downlink burst rate to use an auto-readjust duration of 2 seconds and lowers the IP precedence of violating packets:

```
apn-ambr rate-limit direction downlink burst-size auto-readjust duration 2 violate-action lower-ip-precedence
```
associte accounting-policy

Associates the APN with specific pre-configured policies configured in the same context.

Product
P-GW

Privilege
Administrator

Syntax

[ no ] associte accounting-policy name

----

no
Removes the selected association from this APN.

accounting-policy name
Associates the P-GW APN with an accounting policy configured in the same context. name must be an existing accounting policy and be from 1 to 63 alpha and/or numeric characters. Accounting policies are configured through the policy accounting command in the Context Configuration Mode.

----

Usage
Use this command to associate the P-GW APN with an accounting policy configured in this context.

Example
The following command associates this P-GW APN with an accounting policy called acct1:

associte accounting-policy acct1
authentication

Configures the APN’s authentication parameters.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
authentication [{ msid-auth | imsi-auth [username-strip-apn] [password-use-pco] |
  msisdn-auth [username-strip-apn] [password-use-pco]] [ allow-noauth ][ chap
  preference ][ mschap preference ][ pap preference ]}
```

```
default authentication
```

```
default
Sets the default authentication type for this APN. By default allow-noauth is the type for authentication for an APN.
```

```
msid-auth
Obsolete. Use imsi-auth.
```

```
imsi-auth
Default: Disabled.
Configures the APN to attempt to authenticate the subscriber based on their International Mobile Subscriber Identification (IMSI) number.
```

```
msisdn-auth
Default: Disabled.
Configures the APN to attempt to authenticate the subscriber based on their Mobile Station International Integrated Services Digital Network (MSISDN) number as described in table in Usage section of this command.
```

```
username-strip-apn
Default: Disabled.
This keyword if enabled , either with msisdn-auth or imsi-auth strips the APN name from the user name msisdn@apn or imsi@apn received from AAA and make the user name as msisdn or imsi respectively.
```

```
password-use-pco
Default: Disabled.
This keyword, if enabled, uses the password received through Protocol Configuration Options (PCO) from AAA for authentication.
```

```
allow-noauth
Default: Enabled
Configures the APN to not perform authentication for PDP contexts as described in table in Usage section.
```
### chap preference

Default: Disabled
Configures the APN to attempt to use the Challenge Handshake Authentication Protocol (CHAP) to authenticate the subscriber as described in table in Usage section of this command.
A preference must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. preference must be an integer from 1 through 1000. The lower the integer, the higher the preference.

### mschap preference

Default: Disabled
Configures the APN to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber as described in table in Usage section of this command.
A preference must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. preference must be an integer from 1 through 1000. The lower the integer, the higher the preference.

### pap preference

Default: Disabled
Configures the APN to attempt to use the Password Authentication Protocol (PAP) to authenticate the subscriber as described in table in Usage section of this command.
A preference must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. preference must be an integer from 1 through 1000. The lower the integer, the higher the preference.

### Usage

Use this command to specify how the APN profile should handle PDP context authentication and what protocols to use (if any). The ability to configure this option is provided to accommodate the fact that not every MS will implement the same authentication protocols.
The authentication process varies depending on whether the PDP context is of type IP or PPP. Table given in this section describes these differences.
For IP PDP contexts, the authentication protocol and values will be passed from the SGSN as Protocol Configuration Options (PCOs) within the create PDP context PDU to the GGSN. The GGSN requires that the authentication protocol is specified by this command (with no regard to priority) and will use this information to authenticate the subscriber.

### Table 6. Authentication Process Variances Between PDP Context Type

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>IP PDP Context Behavior</th>
<th>PPP PDP Context Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-noauth</td>
<td>Allows the session even if the PCOs do not match any of the configured algorithms. If there was no match and the aaa constructed-nai authentication parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber’s MSISDN as the username.</td>
<td>Allows the session with no authentication algorithm selected. If the aaa constructed-nai authentication parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber’s MSISDN as the username.</td>
</tr>
</tbody>
</table>
### Authentication Mechanism

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>IP PDP Context Behavior</th>
<th>PPP PDP Context Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>chap</strong></td>
<td>If also specified in the PCOs, this protocol will be used to authenticate the subscriber.</td>
<td>Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.</td>
</tr>
<tr>
<td><strong>mschap</strong></td>
<td>If also specified in the PCOs, this protocol will be used to authenticate the subscriber.</td>
<td>Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.</td>
</tr>
<tr>
<td><strong>pap</strong></td>
<td>If also specified in the PCOs, this protocol will be used to authenticate the subscriber. If this protocol is used is specified and the <code>allow-noauth</code> parameter is disabled, the system will attempt to use the APN’s default username/password specified by the <code>outbound</code> command for authentication via PAP.</td>
<td>Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.</td>
</tr>
<tr>
<td><strong>msid-auth</strong></td>
<td>Obsolete. Use <strong>imsi-auth</strong>.</td>
<td>Obsolete. Use <strong>imsi-auth</strong>.</td>
</tr>
<tr>
<td><strong>imsi-auth</strong></td>
<td>Values in the PCOs are ignored. The subscriber’s IMSI is used as the username for PAP authentication. No password is used.</td>
<td>The subscriber’s IMSI is used as the username for PAP authentication. No password is used.</td>
</tr>
<tr>
<td><strong>msisdn-auth</strong></td>
<td>Values in the PCOs are ignored. The subscriber’s MSISDN is used as the username for PAP authentication. No password is used.</td>
<td>Option not available.</td>
</tr>
</tbody>
</table>

**Example**

The following command would configure the system to attempt subscriber authentication first using MSCHAP, then CHAP, and finally PAP. Since the `allow-noauth` command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be still be allowed access.

```
authentication mschap 1 chap 2 pap 3 allow-noauth
```

To enable **imsi-auth** or **msisdn-auth**, the following command instances must be issued:

```
authentication imsi-auth authentication msisdn-auth
```
bearer-control-mode

This command enables/disables the bearer control mode for network controlled QoS (NCQoS) through this APN. It also controls the sending of IE in GTP messages.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

bearer-control-mode [ ms-only | mixed | none ]
default bearer-control-mode

default
Sets the bearer control mode to default mode of “none”.

ms-only
Default: Disabled.
This keyword sets the bearer control mode to “MS-only” mode. In this mode bearer will be controlled by User Equipment (UE) side.

mixed
Default: Disabled.
This keyword sets the bearer control mode to “Mixed” mode. In this mode bearer will be controlled by User Equipment (UE) and network side (from GGSN) as well. To enable network controlled QoS this option must be enabled.

none
Default: Enabled.
This keyword sets the bearer control mode to “none” mode. With BCM mode as none, system will not send any BCM mode information, BCM IE and BCM information in protocol configuration option (PCO) IE, in GTPC messages sent by GGSN. This command is useful in networks where AGWs/firewalls do not support unknown optional IEs in GTP message.

Usage

Use this command to enable the QoS through bearer control. This can be done either through MS side or from GGSN and MS both. To enable network requested QoS user need to enable “Mixed” mode for bearer control. With this keyword operator can control sending of BCM information in GTPC messages from GGSN. With MS-Only or Mixed options in this mode system sends BCM information element in every Create PDP Context Response & Unknown PDP Context Request and Response message. It is possible in some networks that AGWs/Firewall drops/rejects GTPC message if there is an Unknown optional IE. To resolve this none option is used so operator can control sending of BCM IE and BCM information in PCO IE in GTPC messages from GGSN.
Example
The following command enables the bearer control from network and MS side for NCQoS.

```
bearer-control-mode mixed
```
**cc-home**

Configures the home subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cc-home behavior bits profile index
```

---

**behavior bits**

Specifies the behavior bit for the home subscriber charging characteristic. `bits` can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

---

**profile index**

Default: 8

Specifies the profile index for the home subscriber charging characteristic. `index` can be configured to any integer value between 0 and 15.

---

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

---

**Usage**

When the GGSN is configured to reject the charging characteristics sent by the SGSN for “home” subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use. Multiple behavior bits can be configured for a single profile index by “Or”ing the bit strings together and convert the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the `cc profile` command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

---

**Example**

The following command configures a behavior bit of 2 (0000 0000 0010) and a profile index of 10 for home subscribers charging characteristics:

```
cc-home behavior 2 profile 10
```

The following command configures the behavior bits 3 (0000 0000 0100) and 5 (0000 0001 0000 bin) and a profile index of 14 for home subscriber charging characteristics:

```
cc-home behavior 14 profile 14
```
cc-roaming

Configures the roaming subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
cc-roaming behavior bits profile index
```

- **behavior bits**
  
  Specifies the behavior bit for the roaming subscriber charging characteristic. 
  
  *bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

- **profile index**
  
  Default: 8
  
  Specifies the profile index for the roaming subscriber charging characteristic. 
  
  *index* can be configured to any integer value between 0 and 15.

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

Usage

When the GGSN is configured to reject the charging characteristics sent by the SGSN for “roaming” subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use. Multiple behavior bits can be configured for a single profile index by “Or”ing the bit strings together and convert the result to hexadecimal. 

The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit 10 (0010 0000 0000) and a profile index of 10 for roaming subscriber charging characteristics:

```
cc-roaming behavior 200 profile 10
```

The following command configures the behavior bits 9 (0001 0000 0000) and 6 (0000 0010 0000) and a profile index of 14 for roaming subscriber charging characteristics:

```
cc-roaming behavior 120 profile 14
```
cc-sgsn

Specifies the GGSN’s source for charging characteristics (CC) - those configured locally or those received from the SGSN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

cc-sgsn { radius-returned | home-subscriber-use-GGSN | roaming-subscriber-use-GGSN | visiting-subscriber-use-GGSN } +

cc-sgsn { use-GGSN behavior bits profile index[ 0...15 ] [ radius-returned ] }

no cc-sgsn { { radius-returned | home-subscriber-use-GGSN | roaming-subscriber-use-GGSN | visiting-subscriber-use-GGSN } + | [ use-GGSN ] [ radius-returned ] }

no

Causes the GGSN to accept CCs from the SGSN(s) when the no cc-sgsn command is entered with all applicable keywords. Otherwise, no cc-sgsn can be used to turn off one or more of the GGSN sources of CC.

Before entering no cc-sgsn, it is helpful to determine which CC sources have been configured. This can be done with either show configuration or show apn name in Exec Command Mode.

home-subscriber-use-GGSN

Configures the GGSN to use the locally defined charging characteristics for home subscribers, as configured with the APN Configuration Mode cc-home command.

roaming-subscriber-use-GGSN

Configures the GGSN to use the locally defined charging characteristics for roaming subscribers, as configured with the APN Configuration Mode cc-roaming command.

visiting-subscriber-use-GGSN

Configures the GGSN to use the locally defined charging characteristics for visiting subscribers, as configured with the APN Configuration Mode cc-visiting command.

radius-returned

Configures the GGSN to accept charging characteristics returned from the RADIUS server for all subscribers for the APN.

use-GGSN [ behavior bits ] profile index[ 0...15 ]

Configures the GGSN to accept charging characteristics for all subscribers in the APN.
bits specifies the behavior bit for the charging characteristic. This variable can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

index indicates which profile defined with cc profile, in GGSN Service Configuration mode, GGSN uses as a source for CCs. The index can be configured to any integer value from 0 to 15.

use-GGSN keyword can be entered alone or in conjunction with the radius-returned keyword. When entered, this keyword, overrides previous configuration using any of the home, roaming, and/or visiting keywords.

+ 

More than one of the above keywords can be entered within a single command.

Usage

This command specifies whether or not CCs received from the SGSN will be accepted. If they are not accepted, the GGSN will use those that have been configured locally.

The GGSN’s behavior can be configured for the following subscriber types:

- **Home**: Subscribers belonging to the same Public Land Mobile Network (PLMN) as the one on which the GGSN is located.

- **Roaming**: Subscribers that are serviced by a an SGSN belonging to a different PLMN than the one on which the GGSN is located.

- **Visiting**: Subscribers belonging to a different PLMN than the one on which the GGSN is located.

- Any subscriber in the APN.

Example

The following command instructs the GGSN to accept CCs for any subscriber in the APN based on local profile configurations of CCs.

```plaintext
cc-sgsn use-GGSN profile x
```

Assuming the CC source as defined with the previous command, the following command instructs the GGSN to accept CCs supplied by the SGSN(s) and disables the acceptance of CCs supplied by the GGSN for any subscriber within the APN:

```plaintext
no cc-sgsn use-GGSN
```

The following command instructs the GGSN to accept CCs for any subscriber in the APN based on CC information returned from the RADIUS server. This command can be issued after the previous command to expand the possible sources.

```plaintext
cc-sgsn radius-returned
```

The following command disables the acceptance of CCs supplied by the GGSN for visiting and roaming subscribers:

```plaintext
no cc-sgsn roaming-subscriber-use-GGSN visiting-subscriber-use-GGSN
```
**cc-visiting**

Configures the visiting subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cc-visiting behavior bits profile index
```

**behavior bits**

Specifies the behavior bit for the visiting subscriber charging characteristic. 

*bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

**profile index**

Default: 8

Specifies the profile index for the visiting subscriber charging characteristic.

*index* can be configured to any integer value between 0 and 15.

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

**Usage**

When the GGSN is configured to reject the charging characteristics sent by the SGSN for “visiting” subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use. Multiple behavior bits can be configured for a single profile index by “Or”ing the bit strings together and convert the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

**Example**

The following command configures a behavior bit 7 (0000 0100 0000) and a profile index of 10 for visiting subscriber charging characteristics:

```
cc-visiting behavior 40 profile 10
```

The following command configures the behavior bits 1 (0000 0000 0001) and 12 (1000 0000 0000) and a profile index of 14 for visiting subscriber charging characteristics:

```
cc-visiting behavior 801 profile 14
```
content-filtering category

This command enables/disables the specified pre-configured Category Policy Identifier for Category-based Content Filtering support.

Product

All

Privilege

Security Administrator, Administrator

Syntax

content-filtering category policy-id cf_policy_id

no content-filtering category policy-id

no

Disables the previously configured category policy identifier for Content Filtering support to the APN. This is the default setting.

category policy-id cf_policy_id

This command applies the specified content filtering category policy ID, configured in Active Charging Configuration mode, to this APN.

*cf_policy_id* must be a preconfigured category policy ID in Active Charging Configuration Mode.

In case category policy identifier *cf_policy_id* used here is not configured in Active Charging Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

**Important:** Category Policy Id configured through this mode overrides the Category Policy id configured through the `content-filtering category policy-id` command in Rulebase Configuration Mode of Active Charging Service Configuration mode.

Usage

Use this command to enter the Content Filtering Policy Configuration mode and to enable or disable the Content Filtering Category Policy ID for an APN.

**Important:** If Content Filtering Category Policy ID is not specified here the similar command in ACS Rulebase Configuration Mode determines the policy.

Up to 64 different policy identifier can be defined in a Content Filtering support service.

Example

Following command enters the Content filtering Policy Configuration mode and enables the Category Policy Id 101 for Content Filtering support:

```plaintext
content-filtering category policy-id 101
```
**credit-control-group**

This command configures the Credit Control Group to be used for subscribers who use this APN.

**Product**
GGSN, ECS, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
credit-control-group cc_group_name
no credit-control-group
```

- **no**
  Removes the previously configured Credit Control Group from the APN configuration.

- **cc_group_name**
  Specifies the Credit Control Group name.
  `cc_group_name` must be a alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

Use this command to configure the Credit Control Group for this APN.
Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.
Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.

**Example**
The following command configures a Credit Control Group named `testgroup12` to the current APN:

```
credit-control-group testgroup12
```
**data-tunneling ignore df-bit**

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for tunneling used for the Mobile IP data path.

**Product**

GGSN, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
data-tunneling ignore df-bit
no data-tunneling ignore df-bit
```

**Usage**

Use this command to configure a user so that during Mobile IP tunneling the DF bit is ignored and packets are fragmented.

If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header.

In the GGSN, this command also affects the other L3 tunneling options, IP-in-IP and GRE, but does not affect L2TP tunneling.

**Example**

To enable fragmentation of a subscriber’s packets over a MIP tunnel even when the DF bit is present, enter the following command:

```
data-tunneling ignore df-bit
```
data-tunnel mtu

Configures the Maximum Transmission Unit (MTU) for data sent on the IPv6 tunnel between the P-GW and the mobile node.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
data-tunnel mtu bytes

default data-tunnel mtu
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
<th>Returns the command to the default value of 1500.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>mtu bytes</strong></th>
<th>Default: 1500</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specifies the MTU for the IPv6 tunnel between the P-GW and the mobile node. <em>bytes</em> must be an integer between 1280 and 2000.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the MTU for data traffic on the IPv6 tunnel between the P-GW and the mobile node.

**Example**

The following command sets the MTU for IPv6 data traffic to 1400 bytes:

```
data-tunnel mtu 1400
```
dcca origin endpoint

**Description** This command is obsolete. To configure the Diameter Credit Control Origin Endpoint, in the Credit Control Configuration mode, use the `diameter origin endpoint` command.
**dcca peer-select**

Specifies the Diameter credit control primary and secondary host for credit control.

**Product**
GGSN, ECS, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dcca peer-select peer host_name [ realm realm_name ] [ secondary-peer host_name [ realm realm_name ] ]
```

```
no dcca peer-select
```

---

**no**
Removes the previously configured Diameter credit control peer selection.

---

**peer host_name**
A unique name that you specify for the peer.
peer_name must be an alpha and/or numeric string of from 1 through 127 characters. peer_name allows punctuation marks.

---

**secondary-peer host_name**
Specifies a back-up host that is used for fail-over processing. When the route-table does not find an AVAILABLE route the secondary host performs a fail-over processing.

---

**realm realm_name**
The realm_name must be an alpha and/or numeric string of from 1 to 127 characters. The realm may typically be a company or service name. realm_name allows punctuation marks.

---

**Usage**
Use this command to select a Diameter credit control peer and realm.

---

**WARNING:** This configuration completely overrides all instances of diameter peer-select that have been configured within the Credit Control Configuration Mode for an Active Charging service.

---

**Example**
The following command selects a Diameter credit control peer named test and a realm of companyx

```
dcca peer-select test realm companyx
```
default

Sets/restores the default value assigned for the specified parameter.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

default { access-link ip-fragmentation | accounting-mode | authentication | cc-home | cc-roaming | cc-sgsn | cc-visiting | data-tunneling ignore df-bit | dhcp lease-expiration-policy | idle-timeout-activity {take condition off entry below when this clears too} | ip { address { allocation-method } | header-compression | multicast discard | qos-dscp | source-violation } | 13-to-12-tunnel | loadbalance-tunnel-peers | long-duration-action | max-contexts | mobile ip { home-agent | mn-aaa-removal-indication | required | reverse-tunnel } | pdp-type | ppp { data-compression { mode | protocols } | keepalive | min-compression-size | mtu } | proxy-mlp {required | null-username static-homeaddr} | selection-mode | sgsn payload-compression | timeout { absolute | idle | long-duration | qos-renegotiate } | tunnel load-balance }

access-link ip-fragmentation
Restores the APN access-link parameter to its default setting of normal.

accounting-mode
Restores the APN accounting-mode parameter to its default setting of gtp.

authentication
Restores the APN authentication parameter to its default setting of allow-noauth.

cc-home
Restores the cc-home parameter to its default setting of the following:
  • behavior bits: 0x00
  • profile index: 8

cc-roaming
Restores the cc-roaming parameter to its default setting of the following:
  • behavior bits: 0x00
  • profile index: 8

cc-sgsn
Restores the cc-sgsn parameter to its default setting of the following:
  • home-subscriber-use-GGSN : Disabled
  • roaming-subscriber-use-GGSN : Disabled


**visiting-subscriber-use-GGSN**: Disabled

**cc-visiting**
Restores the cc-visiting parameter to its default setting of the following:

- **behavior bits**: 0x00
- **profile index**: 8

**data-tunneling ignore df-bit**
Restores the data-tunneling parameter to its default setting of disabled.

**dhcp lease-expiration-policy**
Restores the dhcp lease-expiration-policy parameter to its default setting of auto-renew.

**idle-timeout-activity**
Sets or restores the session idle-timeout default so it is reset with both uplink and downlink packets.

**ip { address { allocation-method } | header-compression | multicast discard | qos-dscp | source-violation }**
Restores the APN ip parameters to the following default settings:

- **address allocation-method**: local and allow-user-specified enabled
- **header-compression**: Disabled
- **multicast discard**: configures the default multicast settings which is to discard PDUs
- **qos-dscp**: conversational ef streaming af11 interactive af21 background be
- **source-violation**: check enabled, drop-limit 10

**13-to-12-tunnel**
Restores the layer 3-to-layer 2 tunnel address policy parameter to its default setting of validation with no allocation.

**loadbalance-tunnel-peers**
Restores the loadbalance-tunnel-peers parameter to its default setting of random.

**long-duration-action**
Restores the long-duration-action parameter to its default setting of detection.

**max-contexts**
Restores the max-contexts parameter to its default settings of:

- **primary**: 1000000
- **total**: 1000000

**mobile ip { home-agent | mn-aaa-removal-indication | required | reverse-tunnel }**
Restores the APN mobile-ip parameters to the following default settings:

- **home-agent**: No HA address defined
• **mn-aaa-removal-indication**: Disabled
  • **required**: Disabled
  • **reverse-tunnel**: Enabled

**npu qos traffic priority**
Restores the APN NPU QoS parameter to its default setting of Derive from packet DSCP.

**pdp-type**
Restores the APN pdp-type parameter to its default setting of ipv4.

**ppp**
Restores the APN ppp parameters to the following default settings:
  • **data-compression mode**: normal
  • **data-compression protocols**: stac, mppc, deflate
  • **keepalive**: 0
  • **min-compression-size**: 128
  • **mtu**: 1500

**proxy-mip**
Restores the APN proxy-mip required parameter to its default setting of Disabled.
  • **required**: Configures handling of RRQ to enable the acceptance without NAI extension in this APN. Default: Disabled.
  • **null-username static-homeaddr**: Configures handling of RRQ to enable the acceptance without NAI extension in this APN. Default: Disabled.

**qos-renegotiate**
This keyword is obsolete.

**selection-mode**
Restores the APN selection-mode parameter to its default setting of subscribed.

**sgsn payload-compression**
Configures payload compression by SGSN for this APN.

**timeout**
Restores the APN timeout parameters to the following default settings:
  • **absolute**: 0
  • **idle**: 0
  • **load-balance**: 0
  • **qos-renegotiate**: 180 - This keyword is obsolete.

This is the timeout value for the dampening timer during the dynamic QoS renegotiation.
Usage
After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

Example
The following command restores the ppp min-compression-size parameter to its default setting of 128:

```
default ppp min-compression-size
```
dhcp context-name

Configures the name of the context on the system in which Dynamic Host Control Protocol (DHCP) functionality is configured.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dhcp context-name name
no dhcp context-name name
```

- **no**
  Removes a previously configured context name.

- **name**
  The name of a context configured on the system in which one or more DHCP services are configured. It can be from 1 to 79 alpha and/or numeric characters in length and is case sensitive.

**Usage**
If the APN is to support dynamic address assignment via DHCP (either the proxy or relay mode), this parameter must be configured to point the APN to the name of a pre-configured context on the chassis in which one or more DHCP services are configured.
The command can be used to identify a single DHCP service instance within the specified context to use to facilitate the address assignment.

**Example**
The following command configures the APN to look for DHCP services in a context called `dhcp-ctx`:

```plaintext
dhcp context-name dhcp-ctx
```
dhcp lease-expiration-policy

Configures the system’s handling of PDP contexts whose DHCP assigned IP lease has expired.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

dhcp lease-expiration-policy { auto-renew | disconnect }

---

**auto-renew**
Default: Enabled
Configures the system to automatically renew an IP address’ lease when it is about to expire for PDP contexts facilitated by the APN.

**disconnect**
Default: Disabled
Configures the system to automatically release the PDP context when the lease for the IP address associated with that context expires.

---

Usage
Use this command to specify the action the system is to take when leases for IP addresses for PDP contexts that it are currently facilitated by the current APN are about to expire.

---

Example
The following command causes the system to release PDP contexts associated with the current APN when the lease for their DHCP-assigned IP address expires:

```
dhcp lease-expiration-policy disconnect
```
dhcp service-name

Configures the name of a specific DHCP service to use when dynamically assigning IP addresses to PDP contexts using the Dynamic Host Control Protocol.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

dhcp service-name svc_name
no dhcp service-name svc_name

no
Removes a previously configured DHCP service name.

svc_name
Configures the name of the DHCP service instance that is to be used by the current APN for the dynamic assignment of IP addresses to PDP contexts.
The name can be from 1 to 63 alpha and/or numeric characters in length and it case sensitive.

Usage
Use this command to specify a pre-configured DHCP service instance that is to be used by the APN for IP address assignment when the Dynamic Host Control Protocol is used.
The name of the context in which the desired DHCP service is configured must be specified by the parameter.

Example
The following command instructs the APN to use a DHCP service called dhcp1:

   dhcp service-name dhcp1
**dns**

Configures the Domain Name Service (DNS) servers that will be used by the APN for PPP.

**Product**

GGSN, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
dns { primary | secondary } { address }
no dns { primary | secondary } [ dns_address ]
```

**no**

Deletes a previously configured DNS server.

**primary**

Configures the primary DNS server for the APN.

**secondary**

Configures the secondary DNS server for the APN. Only one secondary DNS server can be configured.

**address**

Default: primary = 0.0.0.0, secondary = 0.0.0.0

Configures the IP address of the DNS server. *address* must be expressed in dotted decimal notation.

**dns_address**

Specifies the IP address of the DNS server to remove. *dns_address* must be expressed in dotted decimal notation.

**Usage**

DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.

The configured DNS IP addresses are relayed to the subscriber within IPCP if the PDP type is PPP, or as PCOs (Protocol Configuration Options) if the PDP type is IP.

The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with **ip name-servers** command, or it can be received from AAA server.

When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN has the third preference.
4. DNS values configured at context level with **ip name-servers** command has the last preference.
**Important:** The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

**Example**
The following commands configure a primary DNS server address of 192.168.100.3 and a secondary DNS server address of 192.168.100.4:

```
dns primary 192.168.100.3

dns secondary 192.168.100.4
```
ehrpd-access

Configures the P-GW to exclude IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network, that do not have IPv6 capabilities.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
[ default | no ] ehrpd-access drop-ipv6-traffic
```

Resets this command to its default setting of disabled.

**Usage**

Use this command to exclude IPv6 traffic from being delivered to UEs on the eHRPD network that do not have IPv6 capabilities.
end

Exits the APN configuration mode and returns to the Administrator-Exec mode prompt.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Administrator-Exec mode.
exit

Exits the APN configuration mode and returns to the context configuration mode.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Returns to the context configuration mode.
firewall policy

This command enables/disables Stateful Firewall support for the APN.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
firewall policy firewall-required
{ default | no } firewall policy
```

- **no**
  Disables Stateful Firewall support for this APN.

- **default**
  Configures the default setting for Stateful Firewall support.
  Default: Disabled

- **firewall-required**
  Enables Stateful Firewall support for this APN.

**Usage**
Use this command to enable or disable Stateful Firewall support for this APN.

**Important:** This command is only available in StarOS 8.0. In StarOS 8.1 and later, this configuration is available in the Rulebase Configuration Mode.

**Important:** Unless Stateful Firewall support for this APN is enabled using this command, firewall processing for this APN is disabled.

**Important:** If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

**Example**
The following command enables Stateful Firewall support for this APN:

```bash
firewall policy firewall-required
```

The following command disables Stateful Firewall support for this APN:
no firewall policy
fw-and-nat policy

This command configures the Firewall-and-NAT policy to be used for subscribers who use this APN.

Product
FW, NAT

Privilege
Security Administrator, Administrator

Syntax
fw-and-nat policy fw_natt_policy

{ default | no } fw-and-nat policy

**default**
Specifies that the default Firewall-and-NAT policy configured in the rulebase be used for subscribers who use this APN.

**no**
Disables Firewall and NAT for the APN.

**fw_natt_policy**
Specifies the Firewall-and-NAT policy for the APN.

fw_natt_policy must be an alpha and/or numeric string of 1 through 63 characters in length. Note that this policy will override the default Firewall-and-NAT policy configured in the ACS rulebase.

Usage
Use this command to configure the Firewall-and-NAT policy for the APN. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be used.

**Important:** This command is customer-specific and is only available in StarOS 8.1.

**Important:** This command must be used to configure the Policy-based Firewall-and-NAT feature.

Example
The following command configures a Firewall-and-NAT policy named standard for the APN:

fw-and-nat policy standard
gsm-qos negotiate

Enables negotiation of QoS attribute Reliability Class based on the configuration provided for Service Data Unit (SDU) Error Ratio and Residual Bit Error Ratio (BER) attributes in the APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
gsm-qos negotiate sdu-error-ratio sdu-error-ratio-code [residual-ber residual-ber-code]

[no] gsm-qos negotiate sdu-error-ratio [sdu-error-ratio-code [residual-ber residual-ber-code]]
```

**no**
Disables the configuration for negotiation of QoS attribute reliability class.

**sdu-error-ratio sdu-error-ratio-code**
Enables the negotiation of QoS attribute reliability class based on Service Data Unit (SDU) Error Ratio attributes.

`sdu-error-ratio-code` corresponds to distinct SDU Error ratio values in integer between the range of 1 to 7.

**residual-ber residual-ber-code**
Enables the optional configuration of negotiation of QoS attribute reliability class based on Residual Bit Error Ratio (BER) attributes.

`residual-ber-code` corresponds to distinct Residual Bit Error Ratio values in integer between the range of 1 to 9.

Usage
This command configures the QoS attribute Reliability Class to be negotiated based on the configuration provided for SDU Error Ratio and Residual BER attributes. The derived Reliability Class and the configured values for SDU Error Ratio and Residual BER are sent back in CPC and UPC response.

The mapping for `sdu-error-ratio-code` is as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10-2</td>
</tr>
<tr>
<td>2</td>
<td>7*10-3</td>
</tr>
<tr>
<td>3</td>
<td>10-3</td>
</tr>
<tr>
<td>4</td>
<td>10-4</td>
</tr>
<tr>
<td>5</td>
<td>10-5</td>
</tr>
</tbody>
</table>
Residual BER needs to be specified when SDU Error Ratio is set to codes 1, 2, 3 or 7 (Or, SDU Error Ratio is intended to be set to a value greater than $5 \times 10^{-4}$), for determining the Reliability Class QoS attribute. Otherwise, the Residual BER value received in the Create PDP context request QoS (or UPC request) would be used. The mapping for `residual-ber-code` is as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$5 \times 10^{-2}$</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-2}$</td>
</tr>
<tr>
<td>3</td>
<td>$5 \times 10^{-3}$</td>
</tr>
<tr>
<td>4</td>
<td>$4 \times 10^{-3}$</td>
</tr>
<tr>
<td>5</td>
<td>$10^{-3}$</td>
</tr>
<tr>
<td>6</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>7</td>
<td>$10^{-5}$</td>
</tr>
<tr>
<td>8</td>
<td>$10^{-6}$</td>
</tr>
<tr>
<td>9</td>
<td>$6 \times 10^{-8}$</td>
</tr>
</tbody>
</table>

**Example**
The following commands configure the negotiation of QoS attribute Reliability Class based on Service Data Unit (SDU) Error Ratio 3 attributes in the APN:

```
gsm-qos negotiate sdu-error-ratio 3
```
**gtpp group**

This command enables a configured GTPP server group to an APN for CGF accounting functionality.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp group group_name [ accounting-context ac_context_name ]
[ no | default ] gtpp group group_name
```

- **no**
  Disables the applied GTPP group for specific APN.

- **default**
  Sets / Restores default GTPP server group specified at the context level or in APN template.

- **group_name**
  Specifies the name of server group that is used for authentication/accounting for specific APN.
  `group_name` must be a string of size 1 to 63 character. It must be the same as configured earlier within the same context of APN.

- **accounting-context ac_context_name**
  Specifies the name of an accounting context on the system that processes accounting for PDP contexts handled by this GGSN service for accounting to specific APN.
  `ac_context_name` specifies the name of the context to be used for accounting. The name must be between 1 and 79 alpha and/or numeric characters and is case sensitive.
  Note that if accounting context is not specified here, it uses the GGSN service context or the context configured by the `accounting context` CLI command in GGSN Service Configuration Mode.

**Usage**

This feature provides the GTPP server configurables under GTPP group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual GTPP server group for subscriber in that context. Each server group consists of a list of CGF accounting servers.

In case no GTPP group is applied for the said APN or default APN template, then the default GTPP server group available at context level is applicable for accounting of specific APN.

**Example**

The following command applies a previously configured GTPP server group named `star1` to an APN within the specific context:
The following command disables the applied GTPP server group for the specific APN:

```plaintext
gtpp group star1

no gtpp group star1
```
The command enables/associates a preconfigured secondary GTPP server group to an APN for CGF accounting functionality. By default it is disabled.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gtpp secondary-group group_name [accounting-context actt_ctxt_name]
[no | default] gtpp secondary-group group_name
```

**no**
Disables the configured/associated GTPP secondary group for specific APN.

**default**
Default: Enabled
Restores the default mode for secondary GTPP group for APN template.

**group_name**
Specifies the name of secondary GTPP server group that is used as an alternate for primary GTPP group associated with specific APN for storage of GTPP messages.

**accounting-context actt_ctxt_name**
Specifies the name of an accounting context on the system that processes accounting for PDP contexts handled by this GGSN service for accounting to specific APN.

Usage
Use this feature to provide the secondary GTPP server group support for an APN.
When the secondary GTPP group is configured with this command, the GTPP messages will be duplicated to the secondary servers also.
This secondary group configuration is ignored, if configured `group_name` is same as the primary group. It will also be ignored, if the configured GTPP group `group_name` and/or accounting context `accounting-context` is invalid. In such a case, the call will be established successfully unlike the primary group configuration where the call drops.
In the absence of the configured `accounting-context` context; by default the GGSN service context is chosen.
The secondary group messages are the low priority ones, and thus they are preferred to be purged when there is no room for the new messages.
For more information on GTPP group, refer `gtpp group` command in this guide.

**Example**
The following command applies a previously configured GTPP server group named `star2` to as secondary GTPP group to an APN within the specific context:

```
      gtpp secondary-group star2
```

The following command disables the applied secondary GTPP server group for the specific APN:

```
      no gtpp secondary-group star2
```
**idle-timeout-activity ignore-downlink**

Configures a session idle-timeout to be reset with uplink packets only, or with both uplink and downlink packets.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[no] idle-timeout-activity ignore-downlink

default idle-timeout-activity
```

- **no**
  
  This is the default setting. When set, the downlink traffic is also considered to be an idle timeout activity.

- **default**
  
  Sets or restores the command to the default setting.

**Usage**

If `idle-timeout-activity ignore-downlink` is configured, the downlink traffic will not be used to reset the idle-timeout. Only uplink packets will be able to reset the idle-timeout. By default, `ignore-downlink` is negated by the `no` command so downlink traffic is also used to reset the idle-timeout.

**Example**

The following command causes both uplink and downlink traffic to reset a session idle-timeout:

```
default idle-timeout-activity
```

The following command causes the session idle-timeout to be reset with only uplink packets:

```
idle-timeout-activity ignore-downlink
```
**ims-auth-service**

It applies an IMS authorization service to a subscriber through APN for Gx interface support and functionality.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ims-auth-service auth_svc_name

[ no | default ] ims-auth-service auth_svc_name
```

- **no**
  Disables the applied IMS authorization service for specific APN.

- **default**
  Sets / Restores default state of IMS authorization service, disabled or as specified at the context level or in APN template.

- **auth_svc_name**
  Specifies the name of IMS authorization service name that is used for Gx interface authentication for specific APN.
  `auth_svc_name` must be a string of size 1 to 63 character preconfigured with in the same context of this APN.

**Usage**
This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

**Example**
Following command applies a previously configured IMS authorization service named `gx_interface1` to an APN within the specific context:

```
ims-auth-service gx_interface1
```

Following command disables the applied IMS authorization service `gx_interface1` for the specific APN:

```
no ims-auth-service gx_interface1
```
ip access-group

Configures IPv4/IPv6 access group for the current APN profile.

**Product**
GGSN, ECS, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] ip access-group acl_group_name [in | out]
```

- **no**
  Removes a previously configured IPv4/IPv6 access group association.

- **acl_group_name**
  Specifies the name of the IPv4/IPv6 access group. `acl_group_name` is a configured ACL group and must be an alpha and/or numeric string of 1 to 79 characters.

- **in | out**
  Default: both (in and out)
  Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively.

**Usage**
Use this command to apply a Single IPv4/IPv6 access control list to multiple subscribers via this APN for inbound or outbound IPv4/IPv6 traffic.
If no traffic direction specified the selected access control list will be applied to both direction of traffic.

**Example**
The following command associates the `sampleipv4Group` access group with the current APN profile for both inbound and outbound access.

```
ip access-group sampleipv4Group
```

The following removes the outbound access group flag for `sampleipv4Group`.

```
no ip access-group sampleipv4Group out
```
ip address alloc-method

Configures the method by which this APN will obtain IP addresses for PDP contexts.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip address alloc-method { dhcp-proxy [ prefer-dhcp-options ] | dhcp-relay | local | no-dynamic } [ allow-user-specified ]
```

---

**dhcp-proxy**
Default: Disabled
Configures the APN to assign an IP address received from a DHCP server.

**Important:** If this option is used, the system’s DHCP parameters must be configured.

---

**dhcp-relay**
Default: Disabled
Configures the APN to forward DHCP packets received from the MS to a DHCP server.

**Important:** If this option is used, the system’s DHCP parameters must be configured.

---

**local**
Default: Enabled
Configures the APN to allocate IP addresses from a pool configured in the destination context on the system.

**Important:** If this option is used, the name of the IP address pool from which to allocate addresses must be configured using the `ip address pool-name` command. If no pool name is specified, the system will attempt to allocate an address from any public pool configured in the destination context.

---

**no-dynamic**
Default: Disabled
Disables the dynamic assignment of IP addresses to PDP contexts using this APN. If a PDP context needing an IP address is received by an APN with this option enabled, it will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

---

**prefer-dhcp-options**
Default: Disabled
This keyword, when specified with `dhcp-proxy` for IP address allocation configuration, GGSN will prefer DHCP supplied parameters over values provided by AAA server or by local configuration. This keyword controls following parameters:

- primary and secondary Domain Name Server (DNS) address
- primary and secondary NetBIOS Name Server (NBNS) address

These values will be sent out in PCO IE of GTP Create PDP Response Message whenever MS Requests for them in Create PDP Request Message.

**Important:** This keyword is available only with dhcp-proxy ip allocation method as this functionality is implemented only for GGSN acting as DHCP proxy.

By default, this functionality is disabled. Hence, DNS and NBNS values, if received from DHCP server will not be considered by the GGSN.

`allow-user-specified`

Default: Enabled

Enables support for PDP contexts requesting the use of specific (static) addresses.

**Important:** If this option is not enabled, PDP contexts requesting the use of a static address will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

**Usage**

Use this command to configure the method by which the APN profile will assign IP addresses to PDP contexts.

When the PDP context is being established and the APN name is determined, the system will examine the APN’s configuration profile. Part of that procedure is determining how to handle IP address allocation. Figure in Example section displays the process used by the system to determine how the address should be allocated.

**Example**

The following command configures the APN to dynamically assign an address from a DHCP server and reject PDP sessions with static IP addresses:

```
ip address alloc-method dhcp-proxy
```

The following command configures the APN to reject sessions requesting dynamically assigned addresses and only allow those with static addresses:

```
ip address alloc-method no-dynamic allow-user-specified
```

The following figure provides the IP address allocation process:
**Figure 4. IP Address Allocation Process**

- **Start**
  - Is a user-specified IP address provided?
    - Yes
      - Is allow-user-specified option enabled?
        - Yes
          - Use IP address specified by user
        - No
          - Address available in locally configured static pool?
            - Yes
              - Use assigned IP address
            - No
              - Is authentication required?
                - Yes
                  - IP address provided by authentication server?
                    - Yes
                      - Does pool name match a configured static pool?
                        - Yes
                          - Use IP address from specified pool
                        - No
                          - Does pool name match a configured private pool?
                            - Yes
                              - Use IP address from specified public pool
                            - No
                              - Is local allocation method enabled?
                                - Yes
                                  - Is dhcp-proxy allocation method enabled?
                                    - Yes
                                      - Assign IP address from block received from DHCP server
                                    - No
                                      - System negotiates IP address of 0.0.0.0 with MS
                                        - System receives DHCP packets from MS and forwards them to DHCP server
                                    - No
                                      - Systemrejects session with cause code 220 (DCH, Unknown PDP address or PDP type)
                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                          - Use IP address from specified public pool
                                        - No
                                        - Is dhcp-proxy-agent option enabled?
                                          - Yes
                                            - Systemnegotiates IP address of 0.0.0.0 with MS
                                          - No
                                            - System rejects session with cause code 220 (DCH, Unknown PDP address or PDP type)
                                              - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                - Use IP address from specified public pool
                                              - No
                                              - Is dhcp-proxy allocation method enabled?
                                                - Yes
                                                  - Assign IP address from block received from DHCP server
                                                - No
                                                  - System negotiates IP address of 0.0.0.0 with MS
                                                    - System receives DHCP packets from MS and forwards them to DHCP server
                                                - No
                                                - System rejects session with cause code 220 (DCH, Unknown PDP address or PDP type)
                                                  - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                    - Use IP address from specified public pool
                                                  - No
                                                  - Is dhcp-proxy-agent option enabled?
                                                    - Yes
                                                      - Systemnegotiates IP address of 0.0.0.0 with MS
                                                    - No
                                                      - System rejects session with cause code 220 (DCH, Unknown PDP address or PDP type)
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
                                                        - System rejects session with cause code ALL_DYNAMIC_PDP_ADDR_OCCUPIED
                                                          - Use IP address from specified public pool
                                                        - No
ip address pool

Configures the name of a private IP address pool configured on the system from which to assign an address for a PDP context.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

ip address pool name pool_name
no ip address pool name pool_name

no
Removes a previously configured pool name.

name pool_name
Specifies the name of the private pool configured on the system from which an IP address will be assigned. The name can be from 1 to 31 alpha and/or numeric characters and is case sensitive.

Usage
If the `ip address alloc-method` command is configured to allow the assignment of IP addresses from a local pool configured on the system, this command instructs the system as to which pool should be used. The pool specified by this command must be a private pool configured in the destination context on the system. Please refer to the `ip pool` command in the context configuration mode for information on configuring IP address pools. Multiple APNs can use the same IP address pool if required. In addition, this command could be issued multiple times to allow a single APN to use different address pools.

Example
The following command configures the system to use a pool named `private_pool1` for address allocation:

```
ip address pool private_pool1
```
ip context-name

Configures the name of the destination context to use for subscribers accessing this APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

ip context-name name

no ip context-name name

no
Removes a previously configured context name.

name
Specifies the name of the context through which subscriber data traffic will be routed. name must be from 1 to 79 alpha and/or numeric characters.

Usage
Use this command to specify the name of a destination context configured on the system through which to route all subscriber data traffic. This context will be used for subscribers accessing this APN. If no name is specified, the system will use the context in which the APN is configured as the destination context. When the APN is used to support Mobile IP functionality, this command is used to indicate the context in which the FA service is configured. If no name is specified, the context in which the GGSN service facilitating the subscriber PDP context is used.

Example
The following command configures the system to route subscriber traffic for the APN through a context called isp1:

ip context-name isp1
ip header-compression

Configures IP packet header compression parameters for this APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

ip header-compression vj
no ip header-compression

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables Van-Jacobson header compression.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>vj</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: Enabled</td>
</tr>
<tr>
<td>Enables Van-Jacobson header compression for IP packets.</td>
</tr>
</tbody>
</table>

Usage
IP header compression reduces packet header overhead resulting in more efficient utilization of available bandwidth.

Example
The following command disables packet header compression for the APN:

no ip header-compression
ip hide-service-address

This command is configured on a per-APN basis. It renders the IP address of the GGSN unreachable from MS's using this APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

[ no | default ] ip hide-service-address

---

no

Allows the mobile station to reach the GGSN’s IP address using this APN.

---

default

Does not allow the mobile station to reach the GGSN’s IP address using this APN.

---

Usage

This hides the GGSN’s IP address from the mobile station for security purposes.

---

Example

The following command allows the GGSN’s IP address to be viewed by the mobile station:

no ip hide-service-address
ip local-address

Configures the local-side IP address of the subscriber's point-to-point connection.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

ip local-address ip_address
no ip local-address

no

Removes a previously configured IP local-address.

ip_address

Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed.

ip_address must be expressed in dotted-decimal notation.

Usage

This parameter specifies the IP address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an unnumbered scheme for local-side addresses.

Example

The following command configures a local address of 192.168.1.23 for the MS:

ip local-address 192.168.1.23
ip multicast discard

Configures the IP multicast discard packet behavior.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

[no] ip multicast discard

no

Removes a previously configured IP multicast discard.

Usage

This command specifies if IP multicast discard is enabled or disabled.

Example

The following command enables IP multicast discard for an APN:

ip multicast discard
ip qos-dscp

Configures the quality of service (QOS) differentiated service code point (DSCP) used when sending data packets over the Gi interface.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
ip qos-dscp { { allocation-retention-priority | background | conversational | interactive traffic_priority | streaming } { dscp} } +
```

```
no ip qos-dscp { allocation-retention-priority | background | conversational | interactive | streaming } +
```

`no`
Restores the QoS parameter to its default setting.

```
allocation-retention-priority
```
Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile. `allocation-retention-priority` can be the integers 1, 2, or 3. DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile. Following table shows the DSCP value matrix for `allocation-retention-priority`.

**Table 7. Default DSCP Value Matrix**

<table>
<thead>
<tr>
<th>Allocation Priority</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Handling Priority</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>1</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td>2</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
</tbody>
</table>

**Important:** If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility however, it is recommended that you configure all three values.

```
background
```
Specifies the QoS for traffic patterns in which the data transfer is not time-critical (for example email exchange). This traffic pattern should be the lowest QOS.
**conversational**
Specifies the QOS for traffic patterns in which there is an constant flow of packets in each direction, upstream and downstream. This traffic pattern should be the highest QOS.

**interactive traffic_priority**
Specifies the QOS for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. This traffic pattern should be a higher QOS than the background pattern, but not as high as that for the streaming pattern. 
*traffic_priority* is the 3GPP traffic handling priority and can be the integers 1,2 or 3.

**streaming**
Specifies the QOS for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream. This traffic pattern should be a higher QOS than the interactive pattern, but not as high as that for the conversational pattern.

dscp
Specifies the DSCP for the specified traffic pattern. `dscp` can be configured to any one of the following:

<table>
<thead>
<tr>
<th>dscp</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>af11:</td>
<td>Assured Forwarding 11 per-hop-behavior (PHB)</td>
</tr>
<tr>
<td>af12:</td>
<td>Assured Forwarding 12 PHB</td>
</tr>
<tr>
<td>af13:</td>
<td>Assured Forwarding 13 PHB</td>
</tr>
<tr>
<td>af21:</td>
<td>Assured Forwarding 21 PHB</td>
</tr>
<tr>
<td>af22:</td>
<td>Assured Forwarding 22 PHB</td>
</tr>
<tr>
<td>af23:</td>
<td>Assured Forwarding 23 PHB</td>
</tr>
<tr>
<td>af31:</td>
<td>Assured Forwarding 31 PHB</td>
</tr>
<tr>
<td>af32:</td>
<td>Assured Forwarding 32 PHB</td>
</tr>
<tr>
<td>af33:</td>
<td>Assured Forwarding 33 PHB</td>
</tr>
<tr>
<td>af41:</td>
<td>Assured Forwarding 41 PHB</td>
</tr>
<tr>
<td>af42:</td>
<td>Assured Forwarding 42 PHB</td>
</tr>
<tr>
<td>af43:</td>
<td>Assured Forwarding 43 PHB</td>
</tr>
<tr>
<td>be:</td>
<td>Best effort forwarding PHB</td>
</tr>
<tr>
<td>ef:</td>
<td>Expedited forwarding PHB</td>
</tr>
<tr>
<td>pt:</td>
<td>Pass through (ToS of user packet is not modified)</td>
</tr>
</tbody>
</table>

**Default:**
- background: be
- interactive
- Traffic Priority 1: ef
- Traffic Priority 1: af21
- streaming: af11
- conversational: ef


More than one of the above keywords can be entered within a single command.
DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they’re tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gi interface(s).

The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in following tables respectively:

**Table 8. Class structure for assured forwarding (af) levels**

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>2</td>
<td>Class 1</td>
</tr>
<tr>
<td>3</td>
<td>Class 2</td>
</tr>
<tr>
<td>4</td>
<td>Class 3</td>
</tr>
<tr>
<td>5</td>
<td>Class 4</td>
</tr>
<tr>
<td>6</td>
<td>Express Forwarding (ef)</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

**Example**
The following command configures the DSCP level for the streaming traffic pattern to be `ef`:

```
ip qos streaming ef
```

The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be `ef`, `ef`, `af22`, and `af41`, respectively:

```
ip qos-dscp conversational ef streaming ef interactive af22 background af41
```
ip source-violation

Enables/disables packet source validation for the current APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax
```
ip source-violation { ignore | check [ drop-limit limit ] } [ exclude-from-accounting ]
```

**ignore**
Default: Disabled
Disables source address checking for the APN.

**check [ drop-limit limit ]**
Default: Enabled, limit = 10
Enables the checking of source addresses received from subscribers for violations.

A **drop-limit** can be configured to set a limit on the number of invalid packets that can be received from a subscriber prior to their session being deleted. **limit** can be configured to any integer value between 0 and 1000000. A value of 0 indicates that all invalid packets will be discarded but the session will never be deleted by the system.

**exclude-from-accounting**
Default: Disabled
Excludes the packets identified with IP source violation from the stats generated for accounting records on a basis of configurables.

**Usage**
Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

**Example**
The following command enables source address validation for the APN and configures a drop-limit of 15:
```
   ip source-violation check drop-limit 15
```
**ip user-datagram-tos copy data-tunnel**

This command controls copying of IP TOS octet value from user IPv4/IPv6 datagrams to IP header of GTP data tunnel header.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[no | default] ip user-datagram-tos copy data-tunnel
```

- **no**
  Removes the preconfigured parameter for this command.

- **default**
  Sets the default behavior of this command. By default this function is disabled.

**Usage**
This command needs to copy TOS byte from inner IP header to the outer IP header for RP connection. This functionality will enable SGSN to detect special TOS marking in the outer IP header of GTP tunnel packets and to identify certain packets as control messages.

**Example**
The following command will copy TOS octet in the IP header of datagram to IP header of GTP tunnel encapsulation:

```plaintext
ip user-datagram-tos copy data-tunnel
```
**ipv6 access-group**

This command configures IPv6 access group for the current APN profile which applies a Single ACL to Multiple Subscribers via APN for ipv6 traffic.

**Product**
GGSN, ECS, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] ipv6 access-group group_name [in | out]
```

- **no**
  Removes a previously configured IPv6 ACL applied to a particular APN for IPv6 traffic. As per your requirement at least one of the two (in | out) must be selected for which the ACL will be removed.

- **group_name**
  Specifies the name of the IPv6 access group. group_name must be an alpha and/or numeric string of 1 to 79 characters.

- **[in | out]**
  Default: both (in and out)
  Specifies the access-group as either inbound or outbound by the keywords in and out, respectively.
  If neither of any specified with the base command the specific IPv6 access control list will be applied to both the traffic (downlink and uplink).

**Usage**

Use this command to apply a single IPv6 access control list to multiple subscribers via an APN for inbound or outbound IPv6 traffic.
If no traffic direction specified the selected access control list will be applied to both direction of traffic.

**Example**
The following command associates the sampleipv6Group access group with the current APN profile for both inbound and outbound access:

```
ipv6 access-group sampleipv6Group
```

The following removes the outbound access group flag for sampleipv6Group

```
no ipv6 access-group sampleipv6Group out
```
**ipv6 address prefix-pool**

Configures the IPv6 address prefix pool name to the subscriber session. User can configure up to a maximum of 4 pools per subscriber.

**Product**

GGSN, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ipv6 address prefix-pool value
```

- **value**
  - Default: None
  - The value may be a string size of 1 to 31 characters.

**Usage**

Names the IPv6 address prefix pool.

**Example**

The following command will Configures the IPv6 address prefix pool name ap1_ipv6 to the subscriber session:

```
ipv6 address prefix-pool ap1_ipv6
```
ipv6 dns

Configures the IPv6 Domain Name Service (DNS) servers.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[no] ipv6 dns { primary | secondary } { ipv6_dns_address }
```

no
Deletes a previously configured DNS server.

primary
Configures the primary DNS server for the APN.

secondary
Configures the secondary DNS server for the APN. Only one secondary DNS server can be configured.

ipv6_dns_address
Configures the IP address of the DNS server.

Usage
DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.
The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with `ip name-servers` command, or it can be received from AAA server.
When DNS is requested in PCO configuration, the following preference will be followed for DNS value:
1. DNS Values received from LNS have the first preference
2. DNS values received from RADIUS Server has the second preference
3. DNS values locally configured with APN has the third preference
4. DNS values configured at context level with `ip name-servers` command has the last preference.

Important: The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

Example
The following command provides an example of setting the primary DNS server:

```plaintext
ipv6 dns primary 1:1:1:1:1:1:1:1
```
ipv6 egress-address-filtering

Egress address filtering filters out packets not meant for the mobile interface ID. The GGSN records the source interface ID of all the packets received from the Mobile. When packets sent to the Mobile are received, the destination interface ID is compared against the list of recorded interface IDs and with the local interface-ID assigned to the Mobile during IPv6CP. If no match is found, the packet is dropped.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

[no] ipv6 egress-address-filtering

<table>
<thead>
<tr>
<th>no</th>
<th>Disables IPv6 egress address filtering.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 egress-address-filtering</td>
<td>Enables IPv6 egress address filtering.</td>
</tr>
</tbody>
</table>

Usage
Used to filter packets that arrive from the internet to a particular site.

Example
The following command provides an example disabling egress address filtering:

```
no ipv6 egress-address-filtering
```
ipv6 initial-router-advt

Creates an IPv6 initial router advertisement interval for the current APN.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ipv6 initial-router-advt { interval | num-advts } { value }
default ipv6 initial-router-advt { interval | num-advts }
```

- **default**
  Resets interval or num-advts to their default setting.

- **interval value**
  Default: 3000ms
  The time interval the initial IPv6 router advertisement is sent to the mobile node in milliseconds.
  value is an integer between 100 and 16000 milliseconds.

- **num-advts value**
  Default: 3
  The number of initial IPv6 router advertisements sent to the mobile node.
  value is an integer between 1 to 16.

**Usage**

This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

**Example**

The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```
I3-to-l2-tunnel address policy

Configures the address allocation/validation policy, when subscriber L3 (IPv4/IPv6) sessions are tunneled using a L2 tunneling protocol, such as L2TP.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
I3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alloc-only</td>
<td>Specifies that the system locally allocates and validates subscriber addresses.</td>
</tr>
<tr>
<td>alloc-validate</td>
<td>Specifies that the system allocates addresses for cases in which IP addresses are dynamically assigned. The system does not validate the address specified by the subscriber.</td>
</tr>
<tr>
<td>no-alloc-validate</td>
<td>Specifies that the system does not allocate or validate subscriber addresses locally for such sessions, it passes the address between remote tunnel terminator to the Mobile Node.</td>
</tr>
</tbody>
</table>

Usage

This command can be useful for such tunnels are MIP HA sessions tunneled from the system using a L2TP tunnels or GGSN PDP contexts of type IP tunneled using L2TP to a remote LNS.

Example

The following command configures the system to locally allocate and validate subscriber addresses:

```
I3-to-l2-tunnel address-policy alloc-only
```
loadbalance-tunnel-peers

Configures how tunnel-peers are selected for this APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```shell
load-balancing { balanced | prioritized | random }
```

**balanced**
Default: Disabled
Tunnel-peer selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of peer nodes available.

**prioritized**
Default: Disabled
Tunnel-peer selection is made based on the priority configured for the peer.

**random**
Default: Enabled
Tunnel-peer selection is random in order.

Usage
Use this command to configure the load-balancing algorithm that defines how the tunnel-peers are selected by the APN when multiple peers are configured in the APN.

Example
The following command sets the APN to connect to tunnel-peers in a sequential order:

```shell
load-balancing balanced
```
long-duration-action detection

This command sets the detection of a session that exceeds the long duration timer and sends notification.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
long-duration-action detection
```

`detection`
Default: Enabled
Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior.

Usage
Use this command to detect a session exceeds the limit set by the long duration timer.
Refer to the `timeout idle` and `timeout long-duration` command for information on setting the long duration timer.

Example
Use the following command to enable detecting the session that exceeds the long duration timer:

```
long-duration-action detection
```
long-duration-action disconnection

This command specifies what action is taken when the long duration timer expires.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
long-duration-action disconnection [ suppress-notification ] [ dormant-only ] +
```

**disconnection**
Default: Disabled
Detects a long duration session and disconnects the session after sending SNMP TRAP and CORBA notification.

**suppress-notification**
Default: Disabled
Suppress the SNMP TRAP and CORBA notification after detecting and disconnecting a long duration session.

**dormant only**
Default: Disabled
Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. It sends the SNMP TRAP and CORBA notification after disconnecting a long duration session.

**Usage**
Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.
Refer to the `timeout idle` and `timeout long-duration` command for information on setting the long duration timer.

**Example**
Use the following command to enable disconnecting sessions that exceed the long duration timer:

```
long-duration-action disconnection
```

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP TRAP and CORBA notification:

```
long-duration-action disconnection suppress-notification
```

Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration and send SNMP TRAP and CORBA notification:
**long-duration-action disconnection dormant-only**

Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration without sending any SNMP TRAP and CORBA notification. If the session is idle and the session-idle-time >= inactivity time the session gets disconnected. Even if session is idle when the long-duration timed-out and session-idle time < inactivity time the timer value is reset to idle-timeout time.

**long-duration-action disconnection dormant-only suppress-notification**
max-contexts

Configures the maximum number of PDP contexts (primary and secondary) that can be facilitated by the APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

max-contexts { [per-subscriber secondary secondary_ctx] [primary number total total_number] 
[ default ] max-contexts

per-subscriber secondary secondary_ctx
This keyword specifies the maximum number of secondary PDP contexts that can be facilitated by the APN per primary context (per-subscriber). Subscribers can have primary PDP and secondary PDP contexts - the secondary contexts share the same IP address as the primary.
secondary_ctx can be configured to any integer value from 0 to 10.
Default: 10

primary number
This keyword specifies the maximum number of primary PDP contexts that can be facilitated by the APN.
Subscribers can have primary PDP and secondary PDP contexts - the secondary contexts can be configured using per-subscriber secondary keyword.
number can be configured to any integer value from 1 to 4000000.
Default: 4000000

total total_number
Specifies the maximum total number of PDP contexts (primary and secondary) that can be facilitated by the APN.
total_number can be configured to any integer value from 1 to 4000000.
Default: 4000000

Usage
This parameter can be used to configure a “soft” limit on the number of PDP contexts supported by a single APN.
Soft limits are based on measurements gathered at regular short intervals (several times per minute) as opposed to measurements taken in real-time. Therefore the sampled measurement may not match the actual number of PDP contexts currently being processed. Every PDP context request received is compared against the result of the last sample. If the sample is less than the soft limit configured, the request will be processed. If it is more, the request will be rejected.

Example
The following command specifies that the maximum number of primary PDP contexts the APN can facilitate is 500,000 while the maximum total number is 750,000:

```
max-contexts primary 500000 total 750000
```
**mbms bmsc-profile**

It applies a configured Broadcast-Multicast Service Center (BM-SC) profile to subscribers through APN for Multimedia Broadcast Multicast Service (MBMS) support and functionality.

**Product**  
GGSN, P-GW

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
mbms bmsc-profile name bmsc_profile_name
no mbms bmsc-profile
```

- **no**
  
  Deletes a previously associated BM-SC profile with this APN.

- **bmsc_profile_name**

  Specifies a name for the BM-SC profile already configured in BMSC configuration mode. `bmsc_profile_name` can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-).

**Usage**

Use this command to associate a configured BM-SC profile to use for MBMS contexts with this APN for MBMS feature support.

For more information on BM-SC profile configuration, refer BMSC Profile Configuration Mode. This command also configures the specific BM-SC profile to use for Internet group Management Protocol (IGMP) JOIN requests received from PDP contexts with this APN.

**Example**

Following command applies a previously configured BM-SC profile named `bm_sc_1` to an APN within the specific context.

```
mbms bmsc-profile name bm_sc_1
```
mbms bearer timeout

Configures the session timeout values for the MBMS bearer contexts with this MBMS APN.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mbms bearer timeout [ absolute | idle ] time
[ no | default ] mbms bearer timeout [ absolute | idle ]
```

- **no**
  Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

- **default**
  Set the default value for the followed option for MBMS bearer context timeout.

- **absolute**
  Default: Disabled
  Configures the absolute maximum time an MBMS bearer context may exist in any state (active or idle).

- **idle**
  Default: Disabled
  Configures the maximum amount of time an MBMS bearer context may be idle.

- **time**
  Default: 0
  Measured in seconds, the time can be configured to any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN.

**Usage**

Use this command to limit the amount of time that an MBMS bearer context session can remain connected.

**Example**
The following commands enables an absolute time timeout of 60000 seconds for MBMS bearer context:

```
mbms bearer timeout absolute 60000
```
mbms ue timeout

Configures the session timeout values for the MBMS user equipment (UE) contexts with this MBMS APN.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
mbms ue timeout { absolute | idle } time
[ no | default ] mbms ue timeout { absolute | idle }
```

**no**
Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

**default**
Set the default value for the followed option for MBMS UE context timeout.

**absolute**
Default: Disabled
Configures the absolute maximum time an MBMS UE context may exist in any state (active or idle).

**idle**
Default: Disabled
Configures the maximum amount of time an MBMS UE context may be idle.

**time**
Default: 0
Measured in seconds, the time can be configured to any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN.

**Usage**
Use this command to limit the amount of time that an MBMS UE context session can remain connected.

**Example**
The following commands enables an absolute time timeout of 60000 seconds for MBMS UE context:

```plaintext
mbms bearer timeout absolute 60000
```
mediation-device

Enables the use of a mediation device and specifies the system context to use for communicating with the device.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

mediation-device [context-name context-name] [delay-GTP-response] [no-early-pdus] [no_interims] +

[ no | default ] mediation-device

+ Indicates that more than one of the options can be specified with a single execution of the command.

**no**
Deletes the mediation-device configuration.

**default**
Changes the mediation device to no context-name configured and restores the mediation device’s default properties.

**context-name context-name**
Default: The subscribers destination context.
Configures the mediation VPN context for this APN.
context-name can be from 1 to 79 alpha and/or numeric characters and is case sensitive.
If not specified, the mediation context is same as the destination context of the subscriber.

**delay-GTP-response**
Default: Disabled
When enabled, delays the CPC response until an Accounting Start response is received from the mediation device.

**no-early-pdus**
Default: Disabled
Specifies that the system delays PDUs from the MS until a response to the GGSN’s accounting start request is received from the mediation device. The PDUs are queued if possible, or discarded
If "no-early-PDUs" is enabled, the chassis shall not send uplink/downlink data from/to a MS till it receives the Acct-Rsp Start for the same--from the mediation device. On receiving the Acct-Rsp, pending PDUs are sent out. The chassis shall buffer up to 4 PDUs per call, before it flushes all the PDUs for that call. It is disabled by default.
no-interims
Default: Disabled
Disables sending of interims to the mediation device.

Usage
This command is used to enable mediation device support for the APN. Mediation devices can be either deep-packet inspection servers or transaction control servers. Keywords to this command can be used in combination to each other, depending on configuration requirements.

Example
The following command enables mediation device support for the APN and uses the protocol configuration located in an system context called ggsn1:

```
mediation-device context-name ggsn1
```

```
mediation-device context-name ggsn1 no-interims no-early-pdus
```

```
mediation-device no-early-pdus no-interims
```

```
mediation-device no-interims no-early-pdus
```

The following command enables mediation device support for the APN and uses the protocol configuration located in the subscribers destination context:

```
mediation-device
```
mobile-ip home-agent

Configures the IP address of the home agent (HA) used by the current APN to facilitate subscriber Mobile IP sessions.

Product
GGSN, FA, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
[n]o mobile-ip home-agent ip_address
```

- **no**
  Removes a previously configured HA address.

- **ip_address**
  The IP address of the HA expressed in dotted-decimal notation.

Usage
If the APN is configured to support Mobile IP for all PDP contexts it is facilitating, this command specifies the IP address of the HA that is to be used.

Example
The following command configures an HA IP address of 192.168.1.15:

```
mobile-ip home-agent 192.168.1.15
```
mobile-ip mn-aaa-removal-indication

Configures the system to remove various information elements when relaying Registration Request messages to the HA.

Product
GGSN, FA, P-GW

Privilege
Security Administrator, Administrator

Syntax

[no] mobile-ip mn-aaa-removal-indication

no
Disables this functionality. This is the default setting.

Usage
When this functionality is enabled, the MN-FA challenge and MN-AAA authentication extensions are removed when relaying a Registration Request (RRQ) to the HA.

Example
The following command enables the system to remove information elements from RRQs relayed to the HA:

    mobile-ip mn-aaa-removal-indication
**mobile-ip mh-ha-hash-algorithm**

Designates the encryption algorithm to use.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mobile-ip mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }
```

<table>
<thead>
<tr>
<th>hmac-md5</th>
<th>md5</th>
<th>rfc-2002-md5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: hmac-md5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The encryption algorithms that may be used.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage**
Provides security by encrypting the data.

**Example**
The following command sets encryption for md5:

```
mobile-ip mn-ha-hash-algorithm md5
```
mobile-ip mh-ha-shared-key

Configures the subscriber MN-HA shared key.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
mobile-ip mn-ha-shared-key key

no mobile-ip mn-ha-shared-key
```

**no**
Disables this functionality. This is the default setting.

**key**
The key must be entered as either a string or a hexadecimal number beginning with “0x”.

Usage
Configures a shared key for the APN.

Example
The following command configures a shared key of `sfd23408imi9yn`:

```
mobile-ip mn-ha-shared-key sfd23408imi9yn
```
**mobile-ip mh-ha-spi**

Configures the SPI number.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mobile-ip mh-ha-spi spi_number
[no] mobile-ip mh-ha-spi
```

- **no**
  Disables this functionality. This is the default setting.

- **spi_number**
  The number must be an integer between 256 and 4294967295.

**Usage**
Configures an SPI number for the APN.

**Example**
The following command configures an SPI number of 428856:

```
mobile-ip mh-ha-spi 428856
```
mobile-ip required

Enables support for Mobile IP functionality for all PDP contexts facilitated by the current APN.

**Product**
GGSN, FA, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] mobile-ip required
```

- `no`
  Disables this functionality. This is the default setting.

**Usage**

Mobile IP functionality for IP PDP contexts is only supported at the APN-level. This command enables/disables Mobile IP support for the APN.

When Mobile IP is performed, the system authenticates the subscriber and the Mobile IP FA. If this option is enabled, the system deletes all PDP contexts attempting to access the APN for which a Mobile IP session can not be established.

**Example**
The following command enables Mobile IP support for the current APN:

```
mobile-ip required
```
**mobile-ip reverse-tunnel**

Configures the system to support reverse-tunneling for Mobile IP sessions facilitated by the current APN.

**Product**

GGSN, FA, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[no] mobile-ip reverse-tunnel
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables this functionality. The default is enabled.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable support for Mobile IP reverse tunneling for the APN. Reverse tunneling is enabled by default.

**Example**

The following command enables reverse-tunneling for the APN:

```
mobile-ip reverse-tunnel
```
nai-construction

Configures the NAI construction parameters on a per-APN basis only rather than by per-aaa-group when constructed NAI authentication is enabled.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

nai-construction {imsi | msisdn} [override-null-username] [ encrypted password string | use-shared-secret-password | password string ]

[default | no] nai-construction

default
Enables default method for NAI construction using International Mobile Subscriber Identity (IMSI) for authentication for a user. GGSN constructs NAI using IMSI when no user-name is received.

no
Disables the NAI construction at the APN level.

imsi
Default: Enabled.
Enables NAI construction using IMSI for authentication for a user. GGSN constructs NAI using IMSI when no user-name is received. This is the default setting.

msisdn
Enables NAI construction using Mobile Station International ISDN Number (MSISDN) for authentication for a user. GGSN constructs NAI using MSISDN when no user-name is received.

override-null-username
Enables NAI construction using IMSI/MSISDN for authentication for a user or when empty user name is received.

encrypted password
Specifies an encrypted password is to be used for this NAI-constructed user. string is a string from 0 - 63 characters.

password
Configures the authentication user-password for this NAI-constructed user. password is a string from 0 - 63 characters.
use-shared-secret-password
Specifies use of the RADIUS authentication shared secret password for this NAI-constructed user.

Usage
NAI-construction defines the behavior for construction at the APN level. If defined for a particular APN, this CLI both works independently and overwrites the behavior of aaa constructed-nai defined at the context level for calls involving this APN. Note that NAI construction using IMSI or MSISDN, where either no user name is received or a blank user name is received for authentication, is applicable only when NAI constructed authentication is enabled using **aaa nai-construction authentication** command in context configuration mode.

Example
The following command enables NAI-construction using IMSI as the authentication type with an encrypted password:

```
nai-construction imsi encrypted password string
```
nexthop-forwarding-address

Configures the next hop forwarding address for the APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

nexthop-forwarding-address ip_address
no nexthop-forwarding-address

no
Disables this function. This is the default setting.

ip_address
Configures the IP address of the nexthop forwarding address.

Usage
Use this command to configure the next hop forwarding address for the APN.

Example
The following command configures the next hop forwarding address to 1.1.1.1 using IPv4:

nexthop-forwarding-address 1.1.1.1
no

Enables/Disables the followed option.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax


- **data-tunneling**
  Configure parameters related subscriber data tunneling.

- **dhcp**
  Configures the DHCP related parameters for the APN.

- **dns**
  Disables use of Domain Name Service.

- **ip**
  Configures Internet Protocol (IP) parameters.

- **ipv6**
  Configures ipv6 related parameters
mediation-device
Configures Mediation Device Parameters.

mobile-ip
Configures mobile-ip for the APN.

next-hop-forwarding-address
Configure the nexthop forwarding address for this APN.

nbns
Disables use of NetBios Name Service

outbound
Configures designated apn host password for PDP Type PPP session authentication.

ppp
Disables PPP-related parameters.

proxy-mip
Enables APN's Proxy MIP setting

qos-renegotiate
This keyword is obsolete.
Disables the enabled dynamic QoS renegotiation for the APN.

qos
Configures QoS attributes related to all the PDP context for the APN.

timeout
Configures session timeout values for this APN.

tunnel
Configures layer 2 or layer 3 tunneling for the APN

virtual-apn
Configures virtual APN.

Usage
This key is used to disable or de-activate the configured commands.

Example
The following command disables the mobile IP support for specific APN:

no
no mobile-ip
nbns

Configures and Enables use of NetBios Name Service for the APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

[no] nbns { primary | secondary } IP_address

no
Removes/disables use of a previously configured NetBios Name Service.

primary
Designates primary NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

secondary
Designates secondary/failover NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

IP_address
Specifies the IPv4/IPv6 address expressed in standard notation.

Usage
This command specifies NBNS parameters. The NBNS option is present for both pdp type IP and pdp type PPP for GGSN.
The system can be configured to use NetBios Name Service for the APN.

Example
The following command configures the APN’s NetBios Name Service to primary IP 192.168.1.15.

nbns primary 192.168.1.15
npu qos

Configures an NPU QoS priority queue for packets facilitated by the APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

[no] npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }

- **no**
  Removes a previously configured priority queue.

- **best-effort**
  Assigns the best-effort queue priority. This is the lowest priority.

- **bronce**
  Assigns the bronze queue priority. This is the third-highest priority.

- **derive-from-packet-dscp**
  Default: Enabled
  Specifies that the priority is to be determined from the DSCP field in the packet's TOS octet.

- **gold**
  Assigns the gold queue priority. This is the highest priority.

- **silver**
  Assigns the silver queue priority. This is the second-highest priority.

Usage

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.
The system can be configured to determine the priority of a subscriber packet either based on the configuration of the APN, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).
Refer to the GGSN System Administration and Configuration Guide for additional information on NPU QoS functionality.

Example

The following command configures the APN’s priority queue to be gold:
npu qos traffic priority gold
outbound

Configures the APN host username and password.

**Syntax**

GGSN, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

outbound { [ encrypted ] password pwd | username name}

no outbound password

**no**

Removes previously configured outbound information for the APN.

**encrypted**

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

**password pwd**

Specifies the password to use for session authentication.

`pwd` must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**username name**

Specifies the username to use for session authentication.

`name` must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**Usage**

This command can be used to provide a username and password for authentication when the subscriber doesn’t supply one in accordance with 3GPP standards. In addition, it can be used to create a PPP session when using L2TP to tunnel IP PDP contexts.

If only a username is specified using this command, the password is determined based on the setting of the `aaa constructed-nai` command in the Context Configuration mode. That command is also used to determine the password if an outbound username and password are configured for the APN when the `imsi-auth` keyword is specified for the `authentication` command in this mode.

**Example**

The following commands configures an APN username of `ispl` and a password of `secRet1234`.

```
outbound username ispl
```
outbound password secret123.4
pdp-type

Configure the type of PDP contexts that are supported by this APN.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
pdp-type ( ipv4 [ ipv6 ] | ipv6 [ ipv4 ] | ppp )
```

- **ipv4 [ ipv6 ]**
  - Default: Enabled
  - Enables support for IPv4 PDP contexts. Also enables support for IPv6 if the IPv6 optional keyword is entered in this command.

**Important:** Entering both IPv4 and IPv6 in either order enables support for both.

- **ipv6 [ ipv4 ]**
  - Default: Disabled
  - Enables support for IPv6 PDP contexts. Also enables support for IPv4 if the IPv6 optional keyword is entered in this command.

**Important:** Entering both IPv4 and IPv6 in either order enables support for both.

- **ppp**
  - Default: Disabled
  - Enables support for PPP PDP contexts.

**Usage**
IP PDP context types are those in which the MS is communicating with a PDN such as the Internet or an intranet using IP. PPP PDP contexts are those in which PPP or PPP Network Control Protocol (NCP) frames from the MS are either terminated at, or forwarded by the GGSN.
If a session specifies a PDP type that is not supported by the APN, the system rejects the session with a cause code of 220 (DCH, Unknown PDP address or PDP type).

**Example**
The following command configures the APN to support PPP context types:

```plaintext
pdp-type ppp
```
**ppp**

Configures the Point-to-Point Protocol (PPP) options for the current APN.

**Syntax**

GGSN, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
ppp { data-compression { protocols protocols | mode modes } | keepalive seconds | min-compression-size min_octets | mtu max_octets }

no ppp { data-compression protocols | keepalive seconds | mtu }
```

**no**

Resets the option specified to its default setting.

**data-compression { mode modes | protocols protocols}**

Default: all protocols enabled

Configures the data compression or the compression protocol to use for the APN.

**mode modes**: Sets the compression mode to one of the following:

- **normal**: Packets are compressed using the packet history for automatic adjustment and for best compression.
- **stateless**: Each packet is compressed individually.

**protocols protocols**: Sets the compression protocol to one of the following:

- **deflate**: DEFLATE algorithm
- **mppc**: Microsoft Point-to-Point Compression
- **stac**: STAC LZS algorithm

**keepalive seconds**

Default: 30

Specifies the frequency of sending the Link Control Protocol (LCP) keep alive messages. `seconds` must be either 0 or in the range from 5 to 14400.

The special value 0 disables the keep alive messages entirely.

**min-compression-size min_octets**

Default: 128

Specifies the smallest packet to which compression may be applied. `min_octets` must be a value in the range from 0 to 2000.

**mtu max_octets**

Default: 1500

Specifies the maximum transmission unit (MTU) for packets accessing the APN. `max_octets` must be a value in the range from 100 to 2000.
**Important:** The MTU refers to the PPP payload which excludes the 2 PPP octets. Therefore, an MTU of 1500 corresponds to the 3GPP standard MTU of 1502 for GTP packets with PPP payloads.

**Usage**
Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

**Example**
The following command configures the ppp data-compression mode for the APN to be stateless:

```plaintext
ppp data-compression mode stateless
```

The following command configures an MTU of 500 for the APN:

```plaintext
ppp mtu 500
```
proxy-mip

Configures support for Proxy Mobile IP functionality for the APN.

Product
GGSN, FA, P-GW

Privilege
Security Administrator, Administrator

Syntax

proxy-mip { required | null-username static-homeaddr }

[no]

Disables this functionality. This is the default setting.

required
Default: Disabled.
Enables proxy-mip for all subscribers using this APN.

null-username
Default: Disabled.
Configures handling of RRQ to enable the acceptance without NAI extension in this APN.

Usage
This command requires that Proxy Mobile IP functionality be performed for all PDP contexts facilitated by the APN.
When Proxy Mobile IP is performed, the system performs subscriber authentication but not Mobile IP FA authentication. It can be configured to handling of RRQ without NAI extension in an APN.
More information about Proxy Mobile IP support for the GGSN can be found in the System Overview Guide.

Example
The following command causes the system to support Proxy Mobile IP for all PDP contexts facilitated by the APN:

proxy-mip required

The following command will enables the accepting of RRQ without NAI extensions in this APN.

proxy-mip null-username static-homeaddr
qos negotiate-limit

This command configure the QoS profile to provide the peak and committed data rate limits that the GGSN assigns to the APN, and sends to the SGSNs in response to GTP create/update PDP context requests for traffic shaping and policing functionality.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

qos negotiate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ] [ peak-data-rate bps [ committed-data-rate bps ] | committed-data-rate [ peak-data-rate bps ]]

no negotiate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming }]

no
Disables the QoS Profile for the APN.

Important: When no Qos Profile is configured, the system’s default behavior is to use the information provided by the SGSN.

downlink
Apply the specified limits and actions to the downlink (to-Gn direction).

uplink
Apply the specified limits and actions to the uplink (to-Gi direction).

class { background | conversational | interactive traffic_priority | streaming }
Apply the specified limits and actions to PDP contexts of the specified UMTS traffic class. The following classes are supported:

•background : Specifies the QOS for traffic patterns in which the data transfer is not time-critical (for example email exchange). This traffic pattern should be the lowest QOS.

•conversational : Specifies the QOS for traffic patterns in which there is an constant flow of packets in each direction, upstream and downstream. This traffic pattern should be the highest QOS.

•interactive traffic_priority : Specifies the QOS for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. This traffic pattern should be a higher QOS than the background pattern, but not as high as that for the streaming pattern. traffic_priority is the 3GPP traffic handling priority and can be the integers 1, 2 or 3.
**streaming**: Specifies the QoS for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream. This traffic pattern should be a higher QoS than the interactive pattern, but not as high as that for the conversational pattern.

**Important**: If this keyword is omitted, the same values are used for all classes.

**committed-data-rate bps**

Default: See Usage section for this command

The committed data rate (guaranteed-data-rate) in bps (bits per second).

*bps* must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified in table given in this chapter. Note that if a non-permitted value is entered for this parameter, then the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps. In addition, if the configured committed rate is lower than the value configured for the peak-data-rate, then the system uses the configured peak rate for this parameter.

**Important**: System measurements for this value exclude the GTP and outer packet headers. In addition, some traffic classes have both a committed rate and a peak rate, while other traffic classes have just a peak rate. If a committed rate is not applicable (i.e., the traffic class is **background** or **interactive**), then an error occurs if this option is configured. If the committed-rate is applicable (i.e., the traffic class is **conversational** or **streaming**), the values supplied by the SGSN are used if this option is not configured.

**peak-data-rate bps**

Default: See Usage section for this command

Specifies the peak data-rate for the subscriber, in bps (bits per second).

*bps* must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified in table given in this chapter. Note that if a non-permitted value is entered for this parameter, then the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps.

**Usage**

This command configures the APN’s quality of service (QoS) profile. This feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular traffic class. Traffic classes are defined in 3GPP TS 23.107 and are negotiated during PDP context activation. Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that the values for the uplink/downlink committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in table given in this chapter.
Table 9. Permitted Values for Committed and Peak Data Rates in GTP Messages

<table>
<thead>
<tr>
<th>Value (bps)</th>
<th>Increment Granularity (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>From 1000 to 63,000</td>
<td>1,000 (e.g. 1000, 2000, 3000, ... 63000)</td>
</tr>
<tr>
<td>From 64,000 to 568,000</td>
<td>8,000 (e.g. 64000, 72000, 80000, ... 568000)</td>
</tr>
<tr>
<td>From 57,600 to 8,640,000</td>
<td>64,000 (e.g. 576000, 640000, 704000, ... 8640000)</td>
</tr>
<tr>
<td>From 8,700,000 to 16,000,000</td>
<td>100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)</td>
</tr>
</tbody>
</table>

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (i.e. it accepts all of the SGSN-provided values for the PDP context.

**Important:** This command should be used in conjunction with the `max-contexts` command to limit the maximum possible bandwidth consumption by the APN.

Additional information on the QoS traffic shaping functionality is located in the *System Enhanced Feature Configuration Guide*.

Default Values:
The following table displays the default values for each of the traffic classes:

Table 10.

|----------------------------------------|-----------------------------|-----------------------------------|--------------------------------------|-----------------------------|-----------------------------------|---------------------|

|----------------------------------------|-----------------------------|-----------------------------------|--------------------------------------|-----------------------------|-----------------------------------|---------------------|

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 1</th>
<th>Downlink Traffic: Disabled</th>
<th>Peak Data Rate(in bps): 16000000</th>
<th>Committed Data Rate(in bps): n/a</th>
<th>Burst Size(in bytes): 65535</th>
<th>Exceed Action: n/a</th>
<th>Violate Action: drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink Traffic: Disabled</td>
<td>Peak Data Rate(in bps): 8640000</td>
<td>Committed Data Rate(in bps): n/a</td>
<td>Burst Size(in bytes): 65535</td>
<td>Exceed Action: n/a</td>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 2</th>
<th>Downlink Traffic: Disabled</th>
<th>Peak Data Rate(in bps): 16000000</th>
<th>Committed Data Rate(in bps): n/a</th>
<th>Burst Size(in bytes): 65535</th>
<th>Exceed Action: n/a</th>
<th>Violate Action: drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink Traffic: Disabled</td>
<td>Peak Data Rate(in bps): 8640000</td>
<td>Committed Data Rate(in bps): n/a</td>
<td>Burst Size(in bytes): 65535</td>
<td>Exceed Action: n/a</td>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>
## APN Configuration Mode Commands

### qos negotiate-limit

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps): 16000000</td>
<td>Peak Data Rate(in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate(in bps): n/a</td>
<td>Committed Data Rate(in bps): n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes): 65535</td>
<td>Burst Size(in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Class:** Interactive, **Traffic Handling Priority:** 3

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps): 16000000</td>
<td>Peak Data Rate(in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate(in bps): n/a</td>
<td>Committed Data Rate(in bps): n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes): 65535</td>
<td>Burst Size(in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Class:** Background

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps): 16000000</td>
<td>Peak Data Rate(in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate(in bps): n/a</td>
<td>Committed Data Rate(in bps): n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes): 65535</td>
<td>Burst Size(in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Important:** If a “Subscribed” traffic class is received, the system changes the class to “Background” and sets the following parameters: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the “Background” class. The received values are used for responses when traffic policing is disabled.

**Example**
The following command sets an uplink peak data rate of 128000 bps for QoS negotiation limit:

```
qos negotiate-limit direction uplink peak-data-rate 128000
```
**qos rate-limit**

Configure the action on subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing/shaping functionality.

**Product**

GGSN, P-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
qos rate-limit { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ] [ burst-size { bytes | auto-readjust [ duration dur ] } ] [ exceed-action { drop | lower-ip-precedence | transmit } [ violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit } ]] [ violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit } ] [ exceed-action { drop | lower-ip-precedence | transmit } ]
```

```
no qos rate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ]
```

**Important:** When no Qos Profile is configured, the system’s default behavior is to use the information provided by the SGSN.

**downlink**

Apply the specified limits and actions to the downlink (the Gn direction).

**uplink**

Apply the specified limits and actions to the uplink (the Gi direction).

**class { background | conversational | interactive traffic_priority | streaming }**

Apply the specified limits and actions to PDP contexts of the specified UMTS traffic class. The following classes are supported:

- **background:** Specifies the QoS for traffic patterns in which the data transfer is not time-critical (for example email exchange). This traffic pattern should be the lowest QoS.

- **conversational:** Specifies the QoS for traffic patterns in which there is an constant flow of packets in each direction, upstream and downstream. This traffic pattern should be the highest QoS.

- **interactive traffic_priority:** Specifies the QoS for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. This traffic pattern should be a higher QoS than the background pattern, but not as high as that for the streaming pattern. traffic_priority is the 3GPP traffic handling priority and can be the integers 1,2 or 3.
**streaming**: Specifies the QoS for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream. This traffic pattern should be a higher QoS than the interactive pattern, but not as high as that for the conversational pattern.

---

**Important**: If this keyword is omitted, the same values are used for all classes.

`burst-size { bytes | auto-readjust [ duration dur ] }`

Default: See Usage section for this command

The burst size allowed, in bytes for peak data rate and committed data rate. `bytes` must be an integer from 1 through 6000000.

---

**Important**: It is recommended that the minimum value of this parameter be configured to the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate. In addition, if the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

`auto-readjust [ duration dur ]` keyword provides the option to calculate the Burst size dynamically while configuring rate-limit. Whenever this keyword is enabled to calculate burst size GGSN QoS negotiated rate to be enforced for this calculation.

Every time there is a change in the rates (due to update QoS), the burst sizes will be updated accordingly. This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate.

By default this keyword is disabled.

`duration dur` describes the duration of burst in seconds. If duration is not specified this keyword will use 1 second as default value. `dur` must be an integer between 1 through 30.

---

**exceed-action { drop | lower-ip-precedence | transmit }**

Default: See Usage section for this command

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence
- **transmit**: Transmit the packet

---

**violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }**

Default: See Usage section for this command

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence
- **shape [transmit-when-buffer-full]**: Enables the traffic shaping and provides the buffering of user packets when subscriber traffic violates the allowed peak/committed data rate. The `[transmit-when-buffer-full]` keyword allows the packet to be transmitted when buffer memory is full.
- **transmit**: Transmit the packet
More than one of the above keywords can be entered within a single command.

Usage

This command configures the APN’s quality of service (QoS) data rate shaping through traffic policing/shaping. This command enables the actions on subscriber flow exceeding or violating peak/committed data rate allowed. The shaping function also provides an enhanced function to buffer the exceeded user packets in a buffer memory and sends them to the subscriber when subscriber traffic goes below the committed or peak data rate limit.

Important: The user packet buffer function in traffic shaping is not applicable for real-time traffic.

Important: If the exceed/violate action is set to “lower-ip-precedence”, this command may override the configuration of the `ip qos-dscp` command in the GGSN service configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service `ip qos-dscp` command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (i.e. it accepts all of the SGSN-provided values for the PDP context.

Important: This command should be used in conjunction with the `max-contexts` command to limit the maximum possible bandwidth consumption by the APN.

Additional information on the QoS traffic shaping and policing functionality is located in the System Enhanced Feature Configuration Guide.

Default Values:
The following table displays the default values for each of the traffic classes:

<table>
<thead>
<tr>
<th>Class: Conversational</th>
<th>Class: Streaming</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Downlink Traffic</strong>: Disabled</td>
<td><strong>Uplink Traffic</strong>: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 16000000</td>
<td>Committed Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td>Exceed Action: lower-ip-precedence</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

| **Downlink Traffic**: Disabled | **Uplink Traffic**: Disabled |
| Peak Data Rate (in bps): 16000000 | Peak Data Rate (in bps): 8640000 |
| Committed Data Rate (in bps): 16000000 | Committed Data Rate (in bps): 8640000 |
| Burst Size (in bytes): 65535 | Burst Size (in bytes): 65535 |
| Exceed Action: lower-ip-precedence | Exceed Action: lower-ip-precedence |
| Violate Action: drop | Violate Action: drop |
Class: Interactive, Traffic Handling Priority: 1

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps): 16000000</td>
<td>Peak Data Rate(in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate(in bps): n/a</td>
<td>Committed Data Rate(in bps): n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes): 65535</td>
<td>Burst Size(in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

Class: Interactive, Traffic Handling Priority: 2

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps): 16000000</td>
<td>Peak Data Rate(in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate(in bps): n/a</td>
<td>Committed Data Rate(in bps): n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes): 65535</td>
<td>Burst Size(in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

Class: Interactive, Traffic Handling Priority: 3

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps): 16000000</td>
<td>Peak Data Rate(in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate(in bps): n/a</td>
<td>Committed Data Rate(in bps): n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes): 65535</td>
<td>Burst Size(in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

Class: Background

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps): 16000000</td>
<td>Peak Data Rate(in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate(in bps): n/a</td>
<td>Committed Data Rate(in bps): n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes): 65535</td>
<td>Burst Size(in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Important:** If a “Subscribed” traffic class is received, the system changes the class to “Background” and sets the following parameters: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the “Background” class. The received values are used for responses when traffic policing is disabled.

To calculate the burst size dynamically a new optional keyword `auto-readjust [ duration dur ]` is provided with `burst-size` keyword. By default the burst size is fixed if defined in bytes with this command. In other words irrespective of the rate being enforced, burst-size fixed as given in the `burst-size` bytes parameter.

For the need of variable burst size depending on the rate being enforced this new keyword `auto-readjust [ duration dur ]` is provided. Use of this keyword enables the calculation of burst size as per token bucket algorithm calculation as $T = B / R$, where $T$ is the time interval, $B$ is the burst size and $R$ is the Rate being enforced.

It also provides different burst size for Peak and Committed data rate-limiting.

If `auto-readjust` keyword is not used a fixed burst size must be defined which will be applicable for peak data rate and committed data rate irrespective of rate being enforced.
If `auto-readjust` keyword is provided without specifying the duration a default duration of 1 second will be taken for burst size calculation.

**Example**
The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak or committed data-rate bps in uplink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos rate-limit direction uplink violate-action shape transmit-when-buffer-full
```
qos-renegotiate

This keyword is obsolete.
qos traffic-police

Configure the maximum rates for PDP context negotiation and for Traffic Policing functionality.

This command is obsolete. This functionality is now supported through `qos negotiate-limit` and `qos rate-limit` commands.
radius

**Description** This command is obsoleted.
radius group

Description: This command is obsoleted.
radius returned-framed-ip-address

This command sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

radius returned-framed-ip-address 255.255.255.255-policy {accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied}

default radius returned-framed-ip-address 255.255.255.255-policy

default
Set the policy to its default of rejecting calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.

accept-call-when-ms-ip-not-supplied
Accept calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.

reject-call-when-ms-ip-not-supplied
Reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.

Usage
Use this command to set the behavior in the APN when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Example
Use the following command to set the APN to reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address:

radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied
radius returned-username

Product
This command configures the username that is returned in accounting messages. If the username is not available in the Protocol Configuration Options (PCO), then the radius returned username is preferred to the constructed username (imsi@apn, msisdn@apn, or outbound username).

Privilege
Security Administrator, Administrator

Syntax
radius returned-username { override-constructed-username | prefer-constructed-username } default radius returned-username

override-constructed-username
If Radius Server returns a username in the Access-Accept message and username is not available in the Protocol Configuration Options (PCO) and then the new username from the radius server will be used.

prefer-constructed-username
If the username is not available in the PCO, constructed username (imsi@apn, msisdn@apn) will be used irrespective of the username for the Radius Server. This is the default.

default radius returned-username
The default value for the radius returned-username is prefer-constructed-username i.e. constructed username (imsi@apn, msisdn@apn) will be used.

Important: If the username is available in the PCO, then that username will be used irrespective of this CLI (radius returned-username).

Usage
Use this command to configure the username that is returned in accounting messages

Example
Following command sets the default value for the radius returned-username is prefer-constructed-username; i.e. constructed username (imsi@apn, msisdn@apn):

default radius returned-username
restriction-value

Configures the level of restriction to ensure controlled co-existence of the Primary PDP Contexts.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
restriction-value
[ default | no ] restriction-value
```

**value**
A unique number identifying the type of network supported for primary PDP contexts facilitated by this APN. The following values are supported:
- **1**: Value used for WAP or MMS type of networks. This corresponds to APN type public-1.
- **2**: Value used for Internet or PSPDN type of networks. This corresponds to APN type public-2.
- **3**: Value used for corporate customers who use MMS. This corresponds to APN type private-1.
- **4**: Value used for corporate who do not use MMS. This corresponds to APN type private-2.

**default | no**
Default: no restriction-value
Entering either `default` or `no restriction-value` sets the internal value to zero (0) so that connection to any APN is allowed.

**Usage**
Restricts the ability to have connections to public access and certain private APNs as required by the APN configuration. Also allows co-existence of the Primary PDP Contexts in a controlled manner. It does not restrict total number of Primary PDP Context for the user. It also configures a method for preventing hackers in the public domain from using the UE as a router.

Access is provided based on the following rules:
- If `value = 1`, then PDP contexts with restriction values of 0, 1, 2, and/or 3 are allowed
- If `value = 2`, then PDP contexts with restriction values of 0, 1 and/or 2 are allowed
- If `value = 3`, then PDP contexts with restriction values of 0 and/or 1 are allowed
- If `value = 4`, then PDP contexts with no restriction values are allowed
- If `default` or `no` syntax is entered, then no PDP contexts have restriction

In the event that a Maximum APN Restriction value is received from the SGSN as part of a PDP context Create (CPCR) or Update (UPCR) message, the GGSN allows the request based on the following matrix:
- If `maximum = 0`, then allow connection to any APN
- If `maximum = 1`, then allow APN Restriction values of 0, 1, 2, and/or 3
- If `maximum = 2`, then allow APN Restriction values of 0, 1 and/or 2
If maximum = 3, the allow APN Restriction values of 0 and/or 1
If maximum = 4, then always reject
If maximum = anything else, then allow all APN Restriction values (1, 2, 3, and/or 4)

Refer to 3GPP 23.060 version 6.9.0 for more information.

Example
The following command sets the restriction value of the APN to 2:

```
restriction-value 2
```
secondary ip pool

This command specifies a secondary IP pool to be used as backup pool for NAT.

Product
NAT

Privilege
Security Administrator, Administrator

Syntax

secondary ip pool pool_name

no secondary ip pool

no
Removes the previous secondary IP pool configuration.

pool_name
Specifies the secondary IP pool name.

pool_name must be an alpha and/or numeric string of 1 through 31 characters in length.

Usage
Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool configured will be appended to the RADIUS supplied IP pool list / APN provided IP pool list whichever is applicable during call setup.

Important: This command is license dependent, requiring the 600-00-7871 NAT Bypass license. Please contact your local sales representative for more information.

Example
The following command configures a secondary IP pool named test123:

secondary ip pool test123
selection-mode

Configures the level of verification that will be used to ensure a MS’s subscription to use this APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
selection-mode { chosen-by-sgsn | sent-by-ms | subscribed } +
```

- **chosen-by-sgsn**
  Default: Disabled
  The MS’s subscription will not be verified and the APN will be provided by the SGSN.

- **sent-by-ms**
  Default: Disabled
  The MS’s subscription will not be verified and the APN will be provided by the MS.

- **subscribed**
  Default: Enabled
  The MS’s subscription will be verified by the SGSN.

+ 
  More than one of the above keywords can be entered within a single command.

Usage

Use this command to specify the level of verification that will be used to ensure a MS’s subscription to use this APN. This setting must match the corresponding setting on the SGSN. If the two settings are not identical, the GGSN rejects the session with a cause code of 201 (D1H, User authentication failed).

Example

The following command specifies that the MS’s subscription will not be verified and that the APN name will be supplied by the SGSN:

```
selection-mode chosen-by-sgsn
```
timeout

Configures the session timeout values for this APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

timeout { absolute | qos-renegotiate } time

[ no | default ] timeout [ absolute | qos-renegotiate ]

---

no
Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

---

default
Set the default value for the followed option.

---

absolute
Configures the absolute maximum time a session may exist in any state (active or idle).

---

qos-renegotiate
This keyword is obsolete.

---

time
Default:
- absolute = 0 (Disabled)
- qos-renegotiate = 300

Measured in seconds, the time can be configured to any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN.

---

Usage
Use this command to limit the amount of time that a subscriber session can remain connected or QoS renegotiation dampening timer.

---

Example
The following commands enables an absolute time timeout of 60000 seconds:

```
timeout absolute 60000
```
timeout bearer-inactivity

This command configures the bearer inactivity timer and the threshold value of the traffic (uplink + downlink) through an APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

timeout bearer-inactivity time volume-threshold total bytes
[ no | default ] timeout bearer-inactivity

no
Removes the configured bearer inactivity timer values and traffic threshold limit.

default
Sets the bearer inactivity timer to disabled mode.

time
Specifies the timeout duration in second to check inactivity on the bearer. time must be an integer value from 3600 through 2592000.

qos-renegotiate
Configures the dampening timeout value for the QoS renegotiation (in seconds). In event of QoS upgrade specified timeout duration will be ignored and renegotiation will start immediately.

volume-threshold total bytes
The keyword sets the volume threshold in bytes to check the low activity on the bearer. This total volume is sum of the traffic in uplink and downlink direction bytes must be an integer value from 1 through 4294967295.

Usage
Use this command to configures the bearer inactivity timer and the threshold value of the traffic (uplink + downlink) through an APN.

Example
The following commands enables the inactivity time on bearer with timeout duration of 7200 seconds and total traffic volume of 256000 bytes in uplink and downlink direction as threshold:

timeout bearer-inactivity 7200 volume-threshold total 256000
timeout idle

Configures the idle timeout duration for long duration timer for subscriber session.

**Product**
- All

**Privilege**
- Security Administrator, Administrator

**Syntax**
```
timeout idle idle_dur
no timeout idle
```

**no**
Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

**idle_dur**
Default: 0
Designates the maximum duration of the session, in seconds, after the expiry of which the system considers the session as dormant or idle and invokes the long duration timer action. `idle_dur` must be a value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

**Usage**
Use this command to set the idle time duration for subscriber session to determine the dormant session. Refer to the `long-duration-action detection` and `long-duration-action disconnection` command in this chapter for additional information.

**Example**
Following command sets the idle timeout duration to 450 seconds.
```
timeout idle 450
```
timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
timeout long-duration ldt_timeout [ inactivity-time inact_timeout ]
no timeout long-duration
```

---

**no**
Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

---

**long-duration ldt_timeout**
Default: 0
Designates the maximum duration of the session, in seconds, before the system automatically reports/terminates the session.
Specifies the maximum amount of time, in seconds, before the specified timeout action is activated.
`ldt_timeout` must be a value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

---

**inactivity-time inact_timeout**
Specifies the maximum amount of time, in seconds, before the specified session is marked as dormant.
inact_timeout must be a value in the range from 0 through 4294967295.
The special value 0 disables the inactivity time specified.

---

**Usage**
Use this command to set the long duration timeout period and inactivity timer for subscriber session. Reduce the idle timeout to free session resources faster for use by new requests.
Refer to the `long-duration-action detection` and `long-duration-action disconnection` command in this chapter for additional information.

---

**Example**
Following command sets the long duration timeout duration to 300 seconds and inactivity timer for subscriber session to 45 seconds.

```plaintext
timeout long-duration 300 inactivity-time 45
```
tunnel address-policy

This command specifies the address allocation / validation policy for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. This means that GGSN IP address validation could be disabled for specified incoming calls.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
tunnel address-policy { alloc-only | alloc-validate | no.alloc-validate }
default tunnel address-policy
```

| alloc-only |
| IP addresses are allocated locally and no validation is done. |

| alloc-validate |
| Default. The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses. |

| no.alloc-validate |
| No IP address assignment or validation is done for calls coming in via L3 tunnels. Incoming static IP addresses are passed. This allows for the greatest flexibility. |

| default |
| Resets the tunnel address-policy to alloc-validate. |

Usage
This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignment. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.

For calls coming through L2TP tunnels, the command `13-to-12-tunnel address policy` as defined in the APN Configuration mode, will continue to be in effect.

Example
Use the following command to reset the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

Use the following command to disable all IP address validation for calls coming through tunnels:

```
tunnel address-policy no.alloc-validate
```
tunnel gre

Configures Generic Routing Encapsulation (GRE) tunnel parameters between the GGSN and an external gateway for the APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

tunnel gre peer-address peer_address local-address local_addr [ preference num ]

no tunnel gre peer-address peer_address

---

no
Disables GRE tunneling for the APN.

---

peer-address peer_address
Specifies the IP address of the external gateway terminating the GRE tunnel.
peer_address must be expressed in dotted decimal notation.

---

local-address local_addr
Specifies the IP address of the interface in the destination context of the GGSN originating the GRE tunnel.
local_addr must be expressed in dotted decimal notation.

---

preference num
Default: 1
This option can be used to assign a preference to the tunnel.
preference can be configured to any integer value from 1 to 128.

---

Important:
Only one GRE tunnel per APN is supported. Therefore, the preference should always be set to “1”.

Usage
Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the GGSN to an external gateway.

Example
The following command configures the system to encapsulate subscriber traffic using GRE and tunnel it from a local address of 192.168.1.100 to a gateway with an IP address of 192.168.1.225:

```plaintext
tunnel gre peer-address 192.168.1.225 local-address 192.168.1.100 preference 1
```
tunnel ipip

Configures IP-in-IP tunnelling parameters between the GGSN and an external gateway for the APN.

**Product**
GGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
tunnel ipip peer-address peer_address local-address local_addr [ preference num ]

no tunnel ipip
```

---

**no**
Disables IP-in-IP tunneling for the APN.

---

**peer-address peer_address**
Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.
peer_address must be expressed in dotted decimal notation.

---

**local-address local_addr**
Specifies the IP address of the interface in the destination context of the GGSN originating the IP-in-IP tunnel.
local_addr must be expressed in dotted decimal notation.

---

**preference num**
Default: 1
If multiple tunnels will be configured, this option can be used to assign a preference to the tunnel.
preference can be configured to any integer value from 1 to 128.

---

**Usage**

Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN to an external gateway.

---

**Example**
The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of 192.168.1.100 to a gateway with an IP address of 192.168.1.225:

```plaintext
tunnel ipip peer-address 192.168.1.225

local-address 192.168.1.100 preference 1
```
tunnel ipsec

This command configures sessions for the current APN to use an IPSEC tunnel based on the IP pool corresponding to the subscribers assigned ip address.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

    [no] tunnel ipsec use-policy-matching-ip-pool

Usage
Disables the use of the IPSEC policy that matches the IP pool that the assigned IP address relates to.

Example
The following command enables the use of the policy that matches the IP pool address:

    tunnel ipsec use-policy-matching-ip-pool
tunnel l2tp

Configures Layer 2 Tunnelling Protocol (L2TP) parameters between the GGSN and an external gateway for the APN.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

tunnel l2tp [peer-address lns-address [encrypted] secret l2tp_secret] [preference num] [tunnel-context name] [local-address ip-address] [crypto-map map_name [encrypted] isakmp-secret crypto_secret]] [local-hostname hostname]

no tunnel [peer-address lns-address]

no
Disables L2TP, or secure L2TP tunneling for the APN if a specific peer-address is not specified, or, if a peer-address is specified, this keyword removes the peer-address configuration from the APN.

l2tp
Configures the APN to support L2TP tunnels to a peer LNS.

peer-address lns-address
Specifies the IP address of the LNS node that the LAC service connects to.
lns-address must be expressed in dotted decimal notation.

Important: A maximum of four LNS peers can be configured per APN.

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

secret l2tp_secret
Specifies the shared secret (password) between the LAC service (configured on the system) and the LNS node.
l2tp_secret must be from 1 to 127 alpha and/or numeric characters and is case sensitive.

preference num
Default: 1
Specifies the preference of the tunnel if the LAC service communicates with multiple LNS nodes.
preference can be configured to any integer value from 1 to 128.
tunnel-context name

Specifies the name of the destination context on the system in which the LAC service(s) is configured. name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.

Important: If this option is not configured, the system will attempt to determine the name of the destination context from the ip context-name parameter configured for the APN.

local-address ip-address

Specifies the IP address of an interface that is bound to a LAC service. This is a mechanism to dictate which LAC service to use to facilitate the subscriber’s L2TP session. address is the IP address of the interface in dotted decimal notation.

Important: If the address configured does not exist or is not bound to a LAC service, the system will automatically choose a LAC service to use.

local-hostname hostname

This keyword configures LAC-Hostname to be used for the communication with the LNS peer for this APN. When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in APN are considered for the LNS peer selection. When APN Configuration is selected, local-hostname configured with “tunnel l2tp” command in the APN for the LNS peer will be used as a LAC Hostname.

Important: For this configuration to take effect allow aaa-assigned-hostname command, which is used to configure LAC-Hostname based on the “Tunnel-Client-Auth-ID” attribute received from the RADIUS Server, needs to be configured in the LAC Service Configuration mode.

hostname is name of the local host for the LNS peer and must be an alpha and/or numeric string of between 1 through 127 characters. When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in APN will be considered for the LNS peer selection. When APN Configuration is selected, local hostname hostname configured with this command in the APN for the LNS peer will be used as a LAC Hostname.

crypto-map map_name { [ encrypted ] secret crypto_secret }

Configures the IPSec crypto-map policy that is to be associated with this L2TP tunnel configuration for secure L2TP. map_name is the name of a crypto-map policy configured on the system and must be from 1 to 127 alpha and/or numeric characters and is case sensitive. encrypted is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file. secret specifies the secret associated with the crypto-map policy. crypto_secret can be from 0x to 255 bytes.

Usage

This command can be used to configure the GGSN to tunnel subscriber traffic to one or more peer LNSs using L2TP or L2TP with IPSec.
When using L2TP, the system functions as a L2TP access Concentrator (LAC) and tunnels traffic to a peer L2TP Network Server (LNS). LAC functionality is supported through the configuration of LAC Services defined in destination contexts configured on the system.

When using crypt-map policies, the system functions in the same fashion as with L2TP, with the exception that the encapsulated L2TP traffic is further encrypted using IPSec. IPSec functionality is supported through the definition of crypto maps configured in the same destination context as the LAC services.

A maximum of four LNS peers can be configured per APN. If no peer is specified, the system will use the LAC Service(s) configured in the same destination context as the APN.

**Example**

The following command configures L2TP support for the APN. It configures the APN to tunnel traffic to an LNS with an IP address of 192.168.1.50 through a LAC service bound to an interface with an IP address 192.168.1.201 configured in a destination context on the system called pdn1. The shared secret between the system and the LNS is 5496secRet. This will be the only LNS configured so the default preference of 1 will not be changed.

```
tunnel l2tp peer-address 192.168.1.50 secret 5496secRet tunnel-context pdn1 local-address 192.168.1.201
```
virtual-apn

Configures references (or links) to alternative APNs to be used for PDP context processing based on properties of the context. This command also configures the APN properties against which the PDP contexts are compared. This command supports roaming and visiting subscriber also.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

virtual-apn { gcdr apn-name-to-be-included { gn | virtual } | preference priority apn apn_name { domain domain_name | mcc mcc_number mnc mnc_number | ggsn-service svc-name | sgsn-address { ip_address | ip_address/mask } | roaming-mode { home | visiting | roaming } } }

no virtual-apn preference priority

no

Removes a previously configured “virtual” APN.

gcdr apn-name-to-be-included { gn | virtual }

If virtual APN to be used is configured, the virtual APN name is sent in G-CDRs. Provides an option to either send the virtual APN name or the Gn APN name (that comes from the SGSN) in G-CDRs.

gr: the APN received in the Create PDP Context Request message from SGSN

virtual: the APN selected by the GGSN. This is the default.

preference priority

Specifies the order in which the referenced APNs are compared by the system.

priority specifies the order and can be configured to any integer value from 1 (highest priority) to 1000 (lowest priority).

apn apn_name

Specifies the name of an alternative APN configured on the system that is to be used for PDP contexts with matching properties.

apn_name is the name of the alternative APN and can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots ( . ) and/or dashes ( - ).

domain domain_name

Specifies the subscriber’s domain name (realm).

domain_name must be a string of 1 through 79 characters in length, is case sensitive and can contain all special characters.

ggsn-service svc-name

Specifies the name of the GGSN service.
svc-name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

mcc mcc_number
Specifies the mobile country code (MCC) portion of the PLMN’s identifier.
mcc_number is the PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc mnc_number
Specifies the mobile network code (MNC) portion of the PLMN’s identifier.
mnc_number is the PLMN MNC identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.

sgsn-address {ip_address | ip_address/mask}
Specifies SGSN address (or network) for this virtual APN.
ip_address is the IP address of the SGSN in dotted decimal notation.
ip_address/mask is the IP address of the SGSN in dotted decimal notation with network-host mask separation.

roaming-mode { home | visiting | roaming }
Supports separate PDP context processing for roaming, visiting, and home subscribers. It supports separate rule type along with domain, imsi, and sgsn-address types.

Usage
This command simplifies the configuration process for mobile operators allowing them to provide subscribers with access to a large number of packet data networks, characterized by APN templates, while only having to configure a small number of APNs on the HLR.
Each “virtual” APN is a reference, or a link, to an alternate APN configured on the system. Each reference is configured with a rule that subscriber PDP contexts are compared against and a priority that dictates the comparison order. The references works as follows:
1. A Create PDP Context Request message is received by the GGSN. The message specifies an APN configured in the HLR.
2. The GGSN determine whether its own matching APN configuration contains “virtual” APN references.
3. The system determines the priority of the references and compares the associated information pertaining to the PDP context against the configured rules.
4. If the rule matches, the parameters in the APN specified by the reference are applied to the PDP context. If not, the rules in the reference with the next highest priority are compared against the PDP context. This occurs until a match is found. If none of the references match, then the parameters within the current APN are applied to the PDP context.
The GGSN supports a maximum of 1023 Virtual APN mapping configurations in a system. A single Gn APN can be configured with up to 1000 mapping rules. Multiple Gn APNs are supported - each requiring Virtual APN mapping configurations. The limit imposed is that the total virtual apn mappings across all Gn APNs should not exceed 1023.
The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular rule (either domain name or mobile country code/mobile network code), the “virtual” APN reference should refer to an APN that not is configured on the system and contain the desired rule. All PDP contexts matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.
Example
The following commands configure two “virtual” APNs, priority 1 references the bigco APN with a domain rule of bigco.com, priority 2 references the bigtown APN with a mobile country code rule of 100 and a mobile network code rule of 50.

```plaintext
virtual-apn preference 1 apn bigco domain bigco.com
virtual-apn preference 2 apn bigtown mcc 100 mnc 50
virtual-apn preference 3 apn bigco.com sgsn-address 192.168.62.2
virtual-apn preference 4 apn bigco.co.kr sgsn-address 192.168.60.2/24
```
Chapter 14
ASN Gateway Service Configuration Mode Commands

The ASN GW Service Configuration Mode is used to create and manage ASN Gateway services within the current context.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

asngw-service name

ASN-GW Service Configuration Mode
```
active-relay

This command enables the active relay functionality for R4 and R6 messages in ASN GW and configures the timeout duration in seconds for R4 or R6 messages actively relayed by the ASN GW (e.g. Data Path messages).

Product
ASN GW

Privilege
Administrator

Syntax

```
active-relay timeout duration
[ default ] active-relay timeout
```

- **default**
  Sets the total timeout duration to 15 seconds to actively relayed R4 or R6 messages.

- **duration**
  Default: 15
  Specifies the maximum allowable timeout duration for the ASN GW service to actively relay the R4 or R6 messages.
  \(duration\) is measured in seconds and can be configured to any integer value from 5 through 65535.

Usage
Use this command to enable the active relay of R4 and R6 messages and also to configure the maximum timeout duration for the actively relayed R4 or R6 messages by ASN GW.
By default system is pre-configured for passive relay functionality for R4 and R6 messages.

Example
The following command configures the timeout duration of 20 seconds for actively relayed R4 or R6 messages:

```
active-relay timeout 20
```
authentication

This command configures the authentication type and parameters used for subscribers in this service.

Product
ASN GW

Privilege
Administrator

Syntax

```
authentication { single-eap | none }

default authentication
```

```
default
Disables the authentication requirement for the ASN GW service.
```

```
single-eap
This keyword enables single Extensible Authentication Protocol (EAP) authentication for specific ASN GW service subscriber. Possible single-EAP authentication are User-only, Device-only, or Device-User authentication.
```

```
none
This is the default setting for authentication. This keyword disables all type of authentications for specific ASN GW service.
```

Usage
Use this command to configure authentication requirements for the ASN GW service.

Example
The following command sets the user authentication for ASN GW service with single EAP:

```
authentication single-eap
```
**bind**

This command binds the ASN GW service to a logical IP interface and configures the maximum number of subscriber supported within an ASN GW service.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
bind address ip_address [ max-subscribers max_subs ]
no bind
```

- **no**
  Removes the binding of the service to a specified interface.

- **ip_address**
  Specifies the IP address of the interface to which the service is being bound. `ip_address` must be expressed in IPv4 dotted decimal or IPv6 colon separated notation.

- **max-subscribers max_subs**
  Configures the maximum number of subscribers allowed to connect with this ASN Gateway within specific ASN GW service.
  `max_subs` must be an integer between 1 and 1500000.

**Usage**

Use this command to associated the service with a specific logical IP address and provides the identity of the ASN Gateway as either the domain name of the ASN GW service or the IP address. This command also configures the maximum number of subscribers can be allowed with this service.

**Example**
The following command binds the ASN GW service to a logical interface with an IP address of `1.2.3.4` with a limit of `250000` subscribers:

```
bind address 1.2.3.4 max-subscribers 250000
```
bs-monitor

This command provides the configurations to enable or disable the ASN base station monitoring and related parameters in a WiMAX ASN.

Product
ASN GW

Privilege
Administrator

Syntax

bs-monitor [ interval duration | num-retry retries | timeout idle_time ]
[ default | no ] bs-monitor

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the configured BS monitoring parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured BS monitoring feature and parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 60</td>
</tr>
<tr>
<td>Configures the interval duration in seconds between two ICMP ping messages sent to ASN BS for BS monitoring.</td>
</tr>
<tr>
<td>duration specifies the amount of time in seconds between two ICMP ping message to monitor an ASN BS and must be an integer value in the range of 1 through 36000.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>num-retry retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 5</td>
</tr>
<tr>
<td>Configures the number of retries before marking specific ASN BS as down/dead.</td>
</tr>
<tr>
<td>retries specifies the number of retries to sent ICMP ping messages to an ASN BS before the ASN BS is declared as dead/unreachable and must be an integer value in the range of 0 through 100.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>timeout idle_time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 3</td>
</tr>
<tr>
<td>Configures the timeout duration to wait for a response from ASN BS of ICMP ping message before retransmitting the ICMP ping packets.</td>
</tr>
<tr>
<td>idle_time must be an integer value in the range of 1 through 10.</td>
</tr>
</tbody>
</table>

Usage

Use this command to enable or disable the base station monitoring and to configure the ASN BS monitoring parameters in a WiMAX ASN.
Important: Base Station Monitoring is a license-enabled feature.

Example
The following command configures the timeout duration of 5 seconds before sending ICMP ping message if ASN BS not responded:
bs-monitor timeout 6
end

This command exits the current mode and returns to the Executive Mode.

Product
All

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Executive mode.
exit

This command exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
This command configures the GRE tunnel parameters for ASN GW gateway functionality within specific ASN GW service.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
gre mtu mtu_size
```

```
default gre mtu
```

- **default**
  Sets the MTU size for GRE tunnel to default value of 1500 bytes in WiMAX network.

- **mtu mtu_size**
  Default: 1500 bytes
  Configures the maximum transmission unit size in bytes in GRE tunnel with specific ASN GW service. 
  *mtu_size* must be an integer between 36 and 2000.

**Usage**
Use this command to support the tunnel reassembly optimization with MTU size in GRE tunnel in WiMAX network.

**Example**
The following command configures the maximum transmission unit (MTU) size to 1700 bytes for GRE tunnel:

```
default gre mtu 1700
```
handover

This command specifies the handover related parameters between BS, ASN GW, and MS.

Product
ASN GW

Privilege
Administrator

Syntax

`handover { anchor { dp-pre-reg-termination timeout duration | dp-termination timeout duration } | max-dp-pre-registrations reg_num | non-anchor { dp-pre-reg-termination timeout duration | dp-termination timeout duration } }`

`default handover { anchor { dp-pre-reg-termination timeout | dp-termination timeout } | max-dp-pre-registrations | non-anchor { dp-pre-reg-termination timeout | dp-termination timeout } }`

-------

**default**
Sets the default values for configured handover parameters.

-------

**anchor**
Configures datapath pre-registration and/or termination parameters for an anchor gateway handover.

-------

**dp-pre-reg-termination timeout duration**
Default: 5
Configures the maximum allowable duration in seconds that a single MS can keep the pre-registration datapath with the previous BS after a handover has completed to another BS.
`duration` is measured in seconds and can be configured to any integer value from 0 through 65535.

-------

**dp-termination timeout duration**
Default: 0
Configures the maximum allowable duration in seconds for which the datapath with the previous BS is maintained after a handover has completed to another BS. The system maintains the old datapath after new datapath setup is completed with another BS for specified period and then terminates it.
`duration` is measured in seconds and can be configured to any integer value from 0 through 65535.

-------

**max-dp-pre-registrations reg_num**
Default: 1
Configures the maximum number of pre-registrations from multiple BSs that a single MS can keep at a time.
`reg_num` is the number of pre-registrations and can be configured to any integer value from 0 through 5.

-------

**non-anchor**
Configures datapath pre-registration and/or termination parameters for a non-anchor gateway handover.
Usage
Use this command to configure the handover related parameters between MS, BS, and ASN GW. By default system is configured to terminate the previous sessions immediately and number of pre-registration from multiple BSs is set to 0 for an MS.

Example
The following command configures the maximum allowable duration as 20 seconds for which the datapath with the previous BS is maintained after a handover has completed to another BS:

```
dp-pre-reg-termination timeout 20
```
idle-mode

Configures the timeout duration in seconds an ASN GW service waits to send a session to the idle mode if no activity occurs for specified duration of entry timeout or reactivate an idle session after the specified duration of exit timeout.

Product
ASN GW

Privilege
Administrator

Syntax
idle-mode { entry-timeout duration } exit-timeout duration | timeout duration }

default idle-mode { entry-timeout | exit-timeout | timeout }

default
Resets the idle mode durations to their respective default values.

no
Disables/removes the configured idle mode entry and/or exit timeout duration for a session.

entry-timeout duration
Default: 60
Specifies the maximum duration in seconds allowed for idle mode entry for a session.
duration is measured in seconds and can be configured to any integer value from 1 through 100000.

exit-timeout duration
Default: 60
Specifies the maximum duration in seconds allowed for session to reenter in to active mode after idle mode exit.
duration is measured in seconds and can be configured to any integer value from 1 through 100000.

timeout duration
Default: 4069
Specifies the maximum time (in seconds) allowed for a session to remain in idle mode. duration must be an integer from 128 to 65535.

Usage
Use this command to configure the ASN GW service to send a session for idle mode or active mode after specified duration of time.

Example
The following command configures the idle mode entry timeout value to 50 seconds:
idle-mode entry-timeout 50
max-retransmission

This command the maximum number of times that the system attempts retransmission of R6 control packets to communicate with unresponsive BS.

Product
ASN GW

Privilege
Administrator

Syntax

**max-retransmission retry**

default max-retransmission

```
default
Sets the maximum number of retransmission counter to 3 for R6 control packets within specific ASN GW service.
```

```
retry
Default: 3
Configures the maximum number of retransmission of R6 control packets to BS before marking it as dead/failed. retry must be an integer between 1 and 10.
```

Usage
Use this command to configure number of retransmission of R6 control packets to BS before marking it as fail/dead.

Example
The following command configures the system to attempt 2 times to send R6 control packets to BS:

```
max-retransmission 2
```
mobile-ip

This command configures Mobile IP support with FA service(s) for specific ASN GW service and specifies the context in which the FA service is configured. Default: no

Product
ASN GW

Privilege
Administrator

Syntax

mobile-ip foreign-agent context context_name

no mobile-ip foreign-agent context

Usage

FA services on the system can be configured either in the same or different contexts from those facilitating ASN GW services. When they are configured in separate contexts, this command configured within an ASN GW service instructs the ASN GW service to route traffic to the context facilitating the FA service. Use the no mobile-ip foreign-agent context to delete a previously configured destination context.

Example

The following command instructs the ASN GW service to use the context named FA-destination for FA functionality:

mobile-ip foreign-agent context fa-destination
peer-asngw

This command provides the facility to configure the addresses of trusted non-anchor ASN GW or non-anchor ASN PC/LR peers that a specific ASN GW service can allow R4 control and data path registration with.

Product
ASN GW

Privilege
Administrator

Syntax

[ no ] peer-asngw address ip_address

no
Removes the configured non-anchor ASN GW or non-anchor ASN PC/LR peers from a specific ASN GW service’s trusted peer list.

address ip_address ip_address
Specifies the IP address of the non-anchor ASN GW or non-anchor ASN PC/LR peers which is added as a trusted peer with the ASN GW service.

ip_address is the IP address of the non-anchor ASN GW or non-anchor ASN PC/LR peers expressed in IPv4 dotted decimal or IPv6 colon separated notation.

Usage
Use this command to create the trusted non-anchor ASN GW or non-anchor ASN PC/LR peers with a specific ASN GW service to establish R4 control and data path registration. On receipt of R4 control or data path registration request message the ASN GW service checks whether non-anchor DPF/Authenticator ASN GW/ASN PC-LR address received in request message is in trusted peer ASN GW/ASN PC-LR list configured with this command. If the Anchor DPF/Authenticator ASN GW/ASN PC-LR address received in request message is not there (or not configured) in non-anchor ASN GW or non-anchor ASN PC/LR peers list the ASN GW service sends response for request message with Failure Indication TLV with unspecified error code. A maximum of 32 ASN GWs or ASN PC/LRs can be configured with this command.

Example
The following command adds the ASN GW with an IP address of 1.2.3.4 as a trusted peer within an ASN GW service.

peer-asngw address 1.2.3.4
policy

This command configures the policies for ASN Gateway behavior within specific ASN GW service.

Product
ASN GW

Privilege
Administrator

Syntax

policy { ms-unexpected-network-reentry | msid-dhcp-chaddr-mismatch | non-anchor-mode } { allow | disallow }

default policy { ms-unexpected-network-reentry | msid-dhcp-chaddr-mismatch | non-anchor-mode }

default

Resets the policy parameters to their respective default values.

---

ms-unexpected-network-reentry

Default: allow
Configures the ASN Gateway to allow/disallow an MS re-entry from the same or a new BS, when an active call already exists for the same MS on the ASN Gateway.
This policy performs in the following manner:
  • If the pre-attachment request of the new call comes from a different BS, re-entry is accepted regardless of the call state.
  • If the pre-attachment request of the new call comes from the same BS, re-entry is accepted if the original call is in any state past the pre-attachment phase.
  • Original call is dropped in favor of new call.

---

msid-dhcp-chaddr-mismatch

Default: disallow
Configures the ASN Gateway to allow/disallow an MS to connect if MSID and DHCP address information mismatched.

---

non-anchor-mode

Default: allow
Configures the ASN Gateway to allow/disallow the creation of non-anchor sessions based on DP Registration Request from any Base Station.
When non-anchor mode is not allowed and a DP Registration Request is received, and there is no matching session for the MSID, the request is rejected and a DP Registration Response is sent with an error code as “Admin Prohibited”.

---

allow

Sets the policies to allow the MS matching with specified policy for ASN Gateway.
disallow
Sets the policies to deny/disallow the MS matching with specified policy for ASN Gateway.

Usage
Use this command to configure the policies for behavior of ASN Gateway to handle the MS connection within specific ASN GW service.

Example
The following command enforce the policy to allow an MS re-entry from new BS, when an active call exists for the same MS on the ASN Gateway via another BS:

```
policy ms-unexpected-network-reentry allow
```
policy asngw-initiated-reauth

This command configures the policies for ASN Gateway behavior to initiate reauthorization triggers from ASN GW service.

Product
ASN GW

Privilege
Administrator

Syntax

policy asngw-initiated-reauth { allow | disallow | max-cmac-key-count max_count | pmk-grace-time grace_time }

default policy asngw-initiated-reauth [ max-cmac-key-count | pmk-grace-time ]

default
Resets the policy to disallow ASN GW initiated re-authorization and sets the default values for CMAC key count and PMK grace time within the specific ASN GW service.

max-cmac-key-count max_count
Default: 100
Configures the ASN Gateway to trigger the reauthorization on the basis of Cipher-based Message Authentication Code (CMAC) key counter. Once the CMAC counter crosses the configured value, the system initiates the reauthorization trigger.

pmk-grace-time grace_time
Default: 60
Configures the ASN Gateway to trigger the reauthorization on the basis of Pairwaise Master Key (PMK) key grace period. Once the configured PMK grace period exhausted the system initiates the reauthorization trigger.

allow
Default: disabled
Configures the ASN Gateway to initiate the reauthorization trigger to start the re-authentication based on two locally configured parameters; i.e. pmk-grace-time and cmac-key-count.

disallow
Default: enabled
Configures the ASN Gateway not to initiate the reauthorization trigger to start the re-authentication based on two locally configured parameters; i.e. pmk-grace-time and cmac-key-count.
Use this command to configure to enable the ASN GW to initiated reauthorization trigger on the basis of configured policy.

**Example**

The following command enforces the policy to trigger the reauthorization from the ASN GW:

```
policy asngw-initiated-reauth allow
```
policy overload

Configures traffic overload policy to control congestion in this service.

Product
ASN GW

Privilege
Administrator

Syntax

policy overload { drop | reject }

default policy overload

default
Sets the traffic overload policy action to reject in this service.

drop
Default: disabled
Specifies that the system is to drop incoming packets containing new session requests.

reject
Default: enabled
Specifies that the system processes new session request messages and responds with a reject message.

Usage
Congestion policies at the service-level can be configured for service. When congestion control functionality is enabled at service level, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Example
The following command configures an overload policy of reject for this ASN GW service:

    policy overload reject
ran-peer-map

Identifies a base station peer map for this service.

Product
ASN GW

Privilege
Administrator

Syntax

`ran-peer-map name`

`no ran-peer-map`

`name`

Specifies the name of the RAN Peer Map. `name` must be from 1 to 31 alpha and/or numeric characters and be an existing peer map. RAN Peer Maps are configured in the Global Configuration Mode.

Usage
Use this command to configure a base station peer map that this service will use to map MAC addresses received in R6 protocol messages to IPv4 addresses.

Example
The following command configures the service to refer to a peer map named `ran12` when reconciling a base station MAC address to an IP address:

`ran-peer-map ran12`
retransmission-timeout

Configures the amount of time that must pass without any response before the system re-attempts to send R6 control packets to BS.

Product
ASN GW

Privilege
Administrator

Syntax

retransmission-timeout duration
[ no | default ] retransmission-timeout

- default
  Sets the timeout duration to 3 seconds for retransmission of R6 control packets.

- no
  Disables/removes the configured timeout duration for retransmission of R6 control packets.

- duration
  Default: 3
  Specifies the maximum allowable time for the ASN GW service to wait for a response from the BS before it (a) attempts to communicate with the BS again (if the system is configured to retry the BS) or (b) marks the BS as unreachable.
  duration is measured in seconds and can be configured to any integer value between 1 and 1,000.

Usage
Use this command in conjunction with the max-retransmission command in order to configure the ASN GW services behavior when it does not receive a response from a particular BS.

Use the no retransmission-timeout command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the default retransmission-timeout command.

The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example
The following command configures a retransmission timeout value of 5 seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:

```
no retransmission-timeout
```
**secondary-ip-hosts**

This command enable/disables the multiple host support behind a WiMAX customer premise equipment (CPE). Default: disabled

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
secondary-ip-hosts max_hosts

default multiple-ip-hosts
```

- **default**
  Sets the multiple host configuration in an ASN GW service to default mode, i.e. disabled.

- **max_hosts**
  Default: 0 (disabled)
  Specifies the maximum number of hosts allowed to connect through one primary node connection behind a WiMAX CPE. `max_hosts` must be an integer from 0 through 4. Where 0, the default value, keeps this feature disabled.

**Usage**
Use this command to enable or disable the multi IP host support in an ASN GW service behind one WiMAX CPE through single primary airlink. If enabled this command supports up to 4 hosts as an auxiliary connection. Accounting and UDR generation for such connection will be based on the primary connection with WiMAX CPE. To apply this facility to a subscriber you need to configure the `ip address secondary-pool` command in the Subscriber Configuration mode.

**Example**
The following command enables the multiple host support and instructs the ASN GW service to allow 3 IP hosts as auxiliary connections behind one CPE:

```
secondary-ip-hosts 3
```

The following command disable the multiple host support and instructs the ASN GW service not to allow auxiliary connections behind one CPE:

```
default secondary-ip-host
```
setup-timeout

Configures the total amount of allowable time for the ASN GW service to setup a connection with the BS before it marks the BS as unreachable.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
setup-timeout duration
```

```
default setup-timeout
```

- **default**
  Sets the total timeout duration to 60 seconds to setup a connection with BS.

- **duration**
  Default: 60
  Specifies the maximum allowable time for the ASN GW service to setup the R6 connection with BS before marks the BS as unreachable.
  `duration` is measured in seconds and can be configured to any integer value between 1 and 100000.

**Usage**
Use this command to configure the maximum setup timeout duration to setup an R6 connection with BS. This command supersedes the duration set through the `max-retransmission` and `retransmission-timeout` commands for R6 connection.
The chassis is shipped from the factory with the connection setup timeout duration to 60 seconds.

**Example**
The following command configures an ASN GW service to mark a BS after waiting for 100 seconds before marks it as dead or unreachable:

```
setup-timeout 100
```
Chapter 15
ASN Paging Controller Configuration Mode Commands

The ASN Paging Controller Configuration Mode is used to create and manage ASN paging and location register services for WiMAX subscribers within a context.
asnpc-id

This command configures the identifier for an ASN Paging Controller for subscribers in this service.

Product
ASN PC-LR

Privilege
Administrator

Syntax

asnpc-id mac_address

default asnpc-id

default
Sets the ASN paging controller identifier as IP address of system running ASN paging controller and location registry service.

mac_address
Specifies the MAC address of the system running ASN paging controller and location registry service. mac_address is the MAC address of paging controller in standard (IEEE 802) format in six groups of two hexadecimal digits, separated by hyphens (-) or colons (:).

Usage
Use this command to configure the MAC address of paging controller for ASN paging controller service.

Example
The following command sets the MAC address of paging controller to 01:23:45:67:89:ab in colon (:) separated format:

asnpc-id 01:23:45:67:89:ab
bind

This command binds the ASN paging controller service to a logical IP interface and configures the maximum number of subscribers allowed within a service.

Product
ASN PC-LR

Privilege
Administrator

Syntax

bind address ip_address [ max-subscribers max_subs ]

no bind

no
Removes the binding of the service to a specified interface.

ip_address
Specifies the IP address of the interface to which the service is being bound. ip_address must be expressed in IPv4 dotted decimal or IPv6 colon separated notation.

max-subscribers max_subs
must be an integer between 0 and 1000000 for an ST16 system.
max_subs must be an integer between 0 and 3000000 for an ASR 5000 system.

Usage
Use this command to associated the service with a specific logical IP address and provides the identity of the ASN paging controller as either the domain name of the ASN paging controller service or the IP address. This command also configures the maximum number of subscribers can be allowed with this service.

Example
The following command binds the ASN paging controller service to a logical interface with an IP address of 1.2.3.4 with a limit of 250000 subscribers:

bind address 1.2.3.4 max-subscribers 250000
end

This command exits the current mode and returns to the Executive Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
```
end
```

Usage
Change the mode back to the Executive mode.
exit

This command exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the previous mode.
max-retransmission

This command configures the maximum number of times that the system attempts retransmission of R6 control packets to communicate with unresponsive BS.

Product
ASN PC-LR

Privilege
Administrator

Syntax

max-retransmission retry

default max-retransmission

default

Sets the maximum number of retransmission counter to 3 for R6 control packets within specific ASN paging controller service.

retry

Default: 3
Configures the maximum number of retransmission of R6 control packets to BS before marking it as dead/failed. retry must be an integer between 1 and 10.

Usage
Use this command to configure number of retransmission of R6 control packets to BS before marking it as fail/dead.

Example
The following command configures the system to attempt 2 times to send R6 control packets to BS:

max-retransmission 2
paging-announce

Configures the number of seconds to wait before sending paging announcement messages to MS.

Product
ASN PC-LR

Privilege
Administrator

Syntax

```
paging-announce timeout duration
```

```
default paging-announce timeout
```

```
default
Sets the paging announce timeout duration to 10 seconds for sending paging announce.
```

```
duration
Default: 10
Specifies the maximum duration in seconds to wait for sending a paging announce to MS.
duration is measured in seconds and must be an integer value from 1 through 1,000.
```

Usage
Use this command to configure the ASN paging controller services to send a paging announce if no data communication is happened for specified duration of time.

Example
The following command configures the paging announce timeout value of 500 seconds:

```
paging-announce timeout 500
```
**paging-group**

This command creates/removes the Paging-Group Identifier within specific ASN paging controller service.

**Product**
ASN PC-LR

**Privilege**
Administrator

**Syntax**

```
paging-group id paging_group_id [ -noconfirm ]
no paging-group id paging_group_id
```

**no**

Disables/removes the Paging Group identifier from specific ASN paging controller service.

**id paging_group_id**

Configures the Paging Group identifier to configure paging agent and other parameters within specific ASN paging controller service.

This is a logical network identifier for the serving BS or other network entity retaining MS service and operational information and/or administering paging activity for the MS while in idle mode. The `paging_group_id` must be an integer from 1 through 65535.

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.

⚠️ **WARNING**: If this keyword option is used with the command the `paging_group_id` will be deleted and disabled with all active/inactive configurations in a paging group without prompting any warning or confirmation.

**Usage**

Use this command to enter/enable/disable Paging Group Identifier Configuration mode functionality within specific ASN paging controller service.

ℹ️ **Important**: A maximum of 32 paging groups can be configured within a service.

**Example**

The following command configures the paging group identifier as **1234** for the ASN paging controller service:

```
paging-group id 1234
```
peer-asngw

This command provides the facility to configure the addresses of trusted anchor ASN GW peers that a specific ASN Paging Controller and Location Registry service will allow R4 control and data path registration with.

Product
ASN PC-LR

Privilege
Administrator

Syntax

[ no ] peer-asngw address ip_address

no
Removes the configured peer anchor ASN GW from a specific ASN PC/LR service’s trusted peer list.

address ip_address
Specifies the IP address of the anchor ASN GW which is added as a trusted peer with the ASN PC/LR service.

ip_address is the IP address of the anchor ASN GW peers expressed in IPv4 dotted decimal or IPv6 colon separated notation.

Usage
Use this command to create the trusted peer anchor ASN GWs with a specific ASN PC/LR service to establish R4 control and data path registration.

On receipt of idle mode entry request message the ASN PC/LR service checks whether the Anchor DPF/Authenticator ASN GW address received in idle mode entry request message is in trusted peer ASN GW list configured with this command. If the Anchor DPF/Authenticator ASN GW address received in idle mode entry request message is not there (or not configured) in peer list the ASN PC/LR service sends idle mode entry response message with Failure Indication TLV with unspecified error code.

A maximum of 32 ASN GWs can be configured with this command.

Example
The following command adds the anchor ASN GW with an IP address of 1.2.3.4 as a trusted peer within an ASN PC service.

peer-asngw address 1.2.3.4
peer-asnpc

This command configures the peer Anchor Paging Controller(s) in this ASN PC/LR service.

**Product**
ASN PC-LR

**Privilege**
Administrator

**Syntax**

```
[ no ] peer-asnpc id mac_address ip-address ip_address
```

- **no**
  Removes the configured peer ASN PC/LR MAC address and IP address as trusted peer anchor ASN PC/LR.

- **id mac_address**
  Specifies the MAC address of the trusted peer system running ASN paging controller and location registry service.
  *mac_address* is the MAC address of paging controller in standard (IEEE 802) format in six groups of two hexadecimal digits, separated by hyphens (-) or colons (:).

- **ip-address ip_address**
  Specifies the IP address of the trusted peer system running ASN paging controller and location registry service.
  *ip_address* is the IP address of paging controller in standard IPv4 format in dotted decimal notation.

**Usage**

Use this command to configure the trusted peer anchor paging controller for ASN paging controller service. This command provides the input for the internal mapping from PC ID to IP address that is needed to forward the Location Update request from new Anchor PC to current Anchor PC during PC relocation.

**Example**

The following command sets the peer AS NPC id to `01:23:45:67:89:ab` in colon (:) separated format and the IP address of the paging controller to `1.1.1.1`:

```
peer-asnpc id 01:23:45:67:89:ab ip-address 1.1.1.1
```
policy overload

Configures traffic overload policy to control congestion in this service.

**Product**
ASN PC-LR

**Privilege**
Administrator

**Syntax**

```
policy overload { drop | reject }
default policy overload
```

```
default
Sets the traffic overload policy action to reject in this service.
```

```
drop
Default: disabled
Specifies that the system is to drop incoming packets containing new session requests.
```

```
reject
Default: enabled
Specifies that the system processes new session request messages and responds with a reject message.
```

**Usage**
Congestion policies at the service-level can be configured for service. When congestion control functionality is enabled at service level, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

**Example**
The following command configures an overload policy of reject for this ASN PC service:

```
policy overload reject
```
retransmission-timeout

Configures the amount of time that must pass without any response before the system re-attempts to send R6 control packets to BS.

Product
ASN PC-LR

Privilege
Administrator

Syntax

```
default
Sets the timeout duration to 3 seconds for retransmission of R6 control packets.

no
Disables/removes the configured timeout duration for retransmission of R6 control packets.

duration
Default: 3
Specifies the maximum allowable time for the ASN paging controller service to wait for a response from the BS before it a) attempts to communicate with the BS again (if the system is configured to retry the BS) or b) marks the BS as unreachable.
duration is measured in seconds and can be configured to any integer value between 1 and 1,000.
```

Usage
Use this command in conjunction with the `max-retransmission` command in order to configure the ASN paging controller services behavior when it does not receive a response from a particular BS.
Use the `no retransmission-timeout` command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the `default retransmission-timeout` command.
The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example
The following command configures a retransmission timeout value of 5 seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:
setup-timeout

Configures the total amount of allowable time for the ASN paging controller service to setup a connection with the BS before it marks the BS as unreachable.

Product
ASN PC-LR

Privilege
Administrator

Syntax

```
setup-timeout duration
default setup-timeout
```

```
default
Sets the total timeout duration to 60 seconds to setup a connection with BS.
```

```
duration
Default: 60
Specifies the maximum allowable time for the ASN paging controller service to setup the R6 connection with BS before marks the BS as unreachable.
duration is measured in seconds and can be configured to any integer value between 1 and 100000.
```

Usage

Use this command to configure the maximum setup timeout duration to setup an R6 connection with BS. This command supersedes the duration set through the `max-retransmission` and `retransmission-timeout` commands for R6 connection.
The chassis is shipped from the factory with the connection setup timeout duration to 60 seconds.

Example

The following command configures an ASN paging controller service to mark a BS after waiting for 100 seconds before marks it as dead or unreachable:

```
setup-timeout 100
```
Chapter 16
ASN Paging Group Configuration Mode Commands

The Paging Group Configuration Mode is used to create and manage Paging Agents for paging and location register controller within the current ASN PC-LR service.

> **Important:** This functionality is still in development stage.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          asnpc-service name
            ASN PC Service Configuration Mode
              paging-group id group_id
                Paging Group Configuration Mode
```
end

This command exits the current mode and returns to the Executive Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```plaintext
end
```

**Usage**
Change the mode back to the Executive mode.
**exit**

This command exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
paging

Configures the paging parameters within the paging group for PC-LR functionality.

Product
ASN PC-LR

Privilege
Administrator

Syntax

```
paging { cycle cycle_value | interval interval_value | node id mac_address
addressip_address | offset algorithm uniform start start_value increment
inc_value count count_value }
```

```
no paging { cycle | node id mac_address | offset }
```

no
Disables the configured paging parameters within this paging group.

cycle cycle_value
Specifies the cycle in which the paging message is transmitted within the paging group. cycle_value must be an integer from 0 through 65535.

interval interval_value
Specifies the maximum duration in frames of Paging Listening Interval; used in calculation of Paging Listening Interval. interval_value must be an integer from 1 through 5.

node id mac_address address ip_address
id mac_address: Configures the MAC address of the node in the paging group. mac_address must be in one of the following formats: nn:nn:nn:nn:nn:nn or nn-nn-nn-nn-nn-nn address ip_address: Specifies the IP address of the node. ip_address must be expressed in IPv4 or IPv6 dotted decimal notation.

```
Important: Up to 128 paging nodes can be configured per paging group.
```

offset algorithm uniform start start_value increment inc_value count
count_value
start start_value: Specifies the starting value of the available offset. start_value must be an integer from 0 through 65535.
increment inc_value: Specifies the distance between two offsets. inc_value must be an integer from 0 through 65535.
count count_value: Specifies the number of offsets available. count_value must be an integer from 0 through 65535.
Offsets are uniformly load balanced across the available range. For this configuration:
The following occurs:
if MS1, MS2,...MS100 perform IM-Entry, then offset assigned would be MS1=10, MS2=20, MS3=30, MS4=40, MS5=10, MS6=20, etc.

Usage
Use this command to define the paging behavior of a paging group. There must be only one instance of paging parameters per paging group.

Example
The following example configures the paging cycle for a paging group to 10.

```
paging cycle 10
```

The following example configures a paging node in the group:
```
paging node id 00:05:47:00:37:44 address 12.345.76.789
```
Chapter 17
ASN QoS Descriptor Configuration Mode Commands

The ASN QoS Descriptor Configuration Mode is used to create and manage Quality of Service Descriptor table for the ASN GW service subscribers within the current source context.
end

This command exits the current mode and returns to the Executive Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Executive mode.
exit

This command exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
**global-service-class-name**

This command configures the global service class name within specific QoS descriptor table.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
global-service-class-name svc_class_name

no global-service-class-name
```

- `no`
  Removes/deletes the configured global service class name from this QoS descriptor table.

- `svc_class_name`
  Specifies the global service class name in QoS descriptor table.
  `svc_class_name` must be an ASCII string of 6 characters in length.

**Usage**

Use this command to specify global service class name as per IEEE 802.16e standard within specific QoS descriptor table for an ASN GW service.

Global Service Class Name is similar in function to the Service Class Name except that (1) Global Service Class Name use may not be modified by a BS, (2) Global Service Class Name remains consistent among all BS, and 3) Global Service Class Names are a rules-based naming system and contains referential QoS parameter codes.

**Example**

The following command specifies the global service class name `g_svc1` in an ASN QoS descriptor table:

```
global-service-class-name g_svc1
```
schedule-type

This command configures the type of data delivery service identifier/type for specific ASN GW service.

Product
ASN GW

Privilege
Administrator

Syntax

schedule-type be [ max-sust_traffic_rate max_sust_traffic_rate | traffic-priority priority_value ] +

schedule-type ert-vr min-reserved-traffic-rate min_resd_traffic_rate max-latency
dur_ms unsolicited-grant-interval dur_ms [ max-sust_traffic_rate
max_sust_traffic_rate | max-traffic-burst burst_size | tolerated-jitter dur_ms |
traffic-priority priority_value ] +

schedule-type nrt-vr min-reserved-traffic-rate min_resd_traffic_rate [ max-
sust_traffic_rate max_sust_traffic_rate | max-traffic-burst burst_size |
traffic-priority priority_value ] +

schedule-type rt-vr min-reserved-traffic-rate min_resd_traffic_rate max-latency
dur_ms unsolicited-polling-interval dur_ms [ max-sust_traffic_rate
max_sust_traffic_rate | max-traffic-burst burst_size | traffic-priority
priority_value ] +

schedule-type ugs min-reserved-traffic-rate min_resd_traffic_rate max-latency
dur_ms unsolicited-grant-interval dur_ms [ sdu-size sdu_size | tolerated-jitter
dur_ms | traffic-priority priority_value] +

default schedule-type

default

Configures the data delivery service type to Best Efforts (BE) service for specific ASN GW service.

be

Configures the data delivery service type to Best Efforts (BE) service for specific ASN GW service.

ert-vr

Configures the data delivery service type to Extended Real-Time Variable Rate (ERT-VR) service for specific ASN GW service.

nrt-vr

Configures the data delivery service type to Non-Real-Time Variable Rate (NRT-VR) service for specific ASN GW service.
### rt-vr
Configures the data delivery service type to Real-Time Variable Rate (RT-VR) service for specific ASN GW service.

### ugs
Configures the data delivery service type to Unsolicited Grant Service (UGS) for specific ASN GW service.

### max-latency `dur_ms`
Specifies the maximum interval in milliseconds between the reception of a packet to BS or SS on its network interface/Convergence Sublayer (CS) and the arrival of packet to its RF interface or the peer device. This value represents a service commitment.

- `dur_ms` must be an integer value between 0 and 65535. Maximum latency set to zero means no commitment available for this service flow.

### min-reserved-traffic-rate `min_resd_traffic_rate`
Default: 0 (disabled)
Specifies the minimum traffic rates in bits per second, reserved for a service flow.

- `min_resd_traffic_rate` must be any integer value between 0 and 65535. Minimum reserved traffic rate set to zero means no minimum traffic rate reservation is required for this service flow.

### max-sustained-traffic-rate `max_sust_traffic_rate`
Configures the maximum sustained traffic rate in bits per second for traffic schedule.

- `traffic_rate` must be an integer between 1 and 65535.

### max-traffic-burst `burst_size`
Default: 0 (disabled)
Specifies the maximum burst size in bits that must be maintained for the service.

- `burst_size` must be any integer value between 0 and 65535. Maximum traffic burst set to zero means no maximum traffic burst reservation is required for this service flow.

### sdu-size `sdu_size`
Default: 49
Specifies the length of the Service Data Unit (SDU) in bytes for a fixed-length SDU service flow.

- `sdu_size` must be any integer value between 1 and 65535.

**Important:** This parameter is used only if packing is on and the service flow is indicated as carrying fixed-length SDUs.

### tolerated-jitter `dur_ms`
Specifies the maximum delay variation (jitter) allowed for the connection.

- `dur_ms` must be any integer value between 1 and 65535.

### traffic-priority `priority_value`
Default: 0 (disabled)
This optional keyword specifies the traffic priority.

- `priority_value` must be an integer from 0 to 7.
unsolicited-grant-interval \textit{dur}\_ms

Specifies the nominal interval in millisecond between successive data grant opportunities for this service flow.
\textit{dur}\_ms must be an integer value between 1 and 65535.

unsolicited-polling-interval \textit{dur}\_ms

Specifies the maximum nominal interval in millisecond between successive polling grants opportunities for this service flow.
\textit{dur}\_ms must be any integer value between 1 and 65535.

Usage

Use this command to configure type of data delivery service identifier within ASN GW service.

\textbf{Important:} Only one data delivery service type between \textit{be}, \textit{et-vr}, \textit{rt-vr}, \textit{nrt-vr}, or \textit{ugs} is allowed within an ASN GW service.

Example

The following command configures the data delivery service type to Best Efforts (BE) service for an ASN GW service:

\texttt{default schedule-type}
service-class-name

This command configures the Service Class Name name within specific QoS descriptor table.

Product
ASN GW

Privilege
Administrator

Syntax

service-class-name svc_class_name

no service-class-name

no
Removes/deletes the configured global service class name from this QoS descriptor table.

svc_class_name
Specifies the service class name in QoS descriptor table.
svc_class_name must be an ASCII string of 2 through 128 characters.

Usage
A Service Class Name is a group of QoS parameters defined at the BS and can be referenced by a service flow to apply certain QoS parameters. Use this command to specify Service Class Name as per IEEE 802.16 standard within specific QoS descriptor table for ASN GW service.

Example
The following command specifies the service class name ASN_Serv_class1 in a ASN QoS descriptor table:

service-class-name ASN_Serv_class1
Chapter 18
ASN RAN Peer Map Configuration Mode Commands

The RAN Peer Map Configuration Mode is used to create and manage global mapping tables of base station peers.

```
Exec Mode
  configure
  Global Configuration Mode
    ran-peer-map
      name
      RAN Peer Map Configuration Mode
```
**end**

This command exits the current mode and returns to the Executive Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```plaintext
eend
```

**Usage**
Change the mode back to the Executive mode.
exit

This command exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.
ran-peer

Configures the MAC and IP addresses of base station peers being added to this map.

Product
ASN GW

Privilege
Administrator

Syntax

[ no ] ran-peer id mac_address address ip_address[mode(non-legacy | legacy)]

no
Removes the base station peer entry from this map.

id mac_address address ip_address

id mac_address: Configures the MAC address of the base station peer in this map.
mac_address must be in one of the following formats:
address ip_address: Specifies the IP address of the base station peer. ip_address must be expressed in IPv4 or IPv6 dotted decimal notation.
mode {non-legacy | legacy}: Default mode is non-legacy.

Usage
Use this command to add base station peers to this peer map.

Example
The following command adds a base station peer to this map:

ran-peer id 00:05:47:00:37:44 address 12.345.76.789
Chapter 19
ASN Service Profile Configuration Mode Commands

The ASN Service Profile Configuration Mode is used to create and manage the service profiles table for the ASN GW service subscribers within the current context.
downlink-classifier

This command specifies the classifier to match for traffic flow in downlink direction for subscribers in this service.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
[ no ] downlink-classifier class-map class_map_name
```

- **no**
  Removes/deletes the configured class map for this traffic flow in the ASN GW service.

- **class-map class_map_name**
  Specifies the configured Class-Map to this traffic flow.
  *class_map_name* is the name of an existing Class-Map configured in the destination context.
  Refer to the Class-Map Configuration Mode chapter of this reference for additional information to configure the class maps.

**Usage**
Use this command to configure classifier for downlink traffic with a configured Class-Map for the ASN GW service subscribers.
A maximum of 4 class-maps can be configured in one ASN GW service profile.
Class-Map Configuration Mode is accessible through Context Configuration Mode.

**Example**
The following command applies the Class-Map *class_1* to this traffic:

```
downlink-classifier class-map class_1
```
downlink-qos-id

This command specifies the QoS table identifier to traffic flow in downlink direction for subscribers in this service.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
downlink-qos-id qos_table_id
[ no ] downlink-qos-id
```

- **no**
  Removes/deletes the configured class map for this traffic flow in the ASN GW service.

- **qos_table_id**
  Specifies the configured ASN QoS Descriptor Identifier to this traffic flow.
  `qos_table_id` is the identifier of an existing ASN QoS Descriptor Table configured in the source context.
  Refer to the ASN QoS Descriptor Configuration Mode chapter of this reference for additional information to configure QoS descriptor table identifier.

**Usage**

Use this command to apply a QoS identifier for downlink traffic with a configured ASN QoS Descriptor Table Identifier for the ASN GW service subscribers.
Only one QoS identifier can be configured in one ASN GW service profile.
ASN QoS Descriptor Configuration Mode is accessible through Context Configuration Mode.

**Example**
The following command applies the QoS table identifier **123** to this traffic:

```
downlink-qos-id 123
```
end

This command exits the current mode and returns to the Executive Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Executive mode.
exit

This command exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the previous mode.
uplink-classifier

This command specifies the classifier to match for traffic flow in uplink direction for subscribers in this service.

Product
ASN GW

Privilege
Administrator

Syntax

[ no ] uplink-classifier class-map class_map_name

no
Removes/deletes the configured class map for this traffic flow in the ASN GW service.

class-map class_map_name
Specifies the configured Class-Map to this traffic flow.
class_map_name is the name of an existing Class-Map configured in the destination context.
Refer to the Class-Map Configuration Mode chapter of this reference for additional information to configure class maps.

Usage
Use this command to configure classifier for uplink traffic with a configured Class-Map for the ASN GW service subscribers.
A maximum of 4 class-maps can be configured in one ASN GW service profile.
Class-Map Configuration Mode is accessible through Context Configuration Mode.

Example
The following command applies the Class-Map class_1 to this traffic:

uplink-classifier class-map class_1
**uplink-qos-id**

This command specifies the QoS table identifier to traffic flow in uplink direction for subscribers in this service.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```plaintext
uplink-qos-id qos_table_id
[ no ] uplink-qos-id
```

- **no**
  Removes/deletes the configured class map for this traffic flow in the ASN GW service.

- **qos_table_id**
  Specifies the configured ASN QoS Descriptor Identifier to this traffic flow.
  `qos_table_id` is the identifier of an existing ASN QoS Descriptor Table configured in the source context. Refer to the ASN QoS Descriptor Configuration Mode chapter of this reference for additional information to configure QoS descriptor table identifier.

**Usage**
Use this command to apply a QoS identifier for uplink traffic with a configured ASN QoS Descriptor Table Identifier for the ASN GW service subscribers.
Only one QoS identifier can be configured in one ASN GW service profile.
ASN QoS Descriptor Configuration Mode is accessible through Context Configuration Mode.

**Example**
The following command applies the QoS table identifier 123 to this traffic:

```plaintext
uplink-qos-id 123
```
Chapter 20
ATM Port Configuration Mode Commands

The Asynchronous Transfer Mode (ATM) port configuration mode provides the commands to create, configure, bind, and manage the ATM ports on line cards that support ATM, such as the ATM/POS OC-3 single-mode and multi-mode optical line cards.

**Important:** Before using these commands, card framing should be configured for either SDH or SONET with the framing command described in the *Card Configuration Mode* chapter.

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

Restores the port’s default speed and communication mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default { preferred slot | threshold { threshold_type } }
```

---

**preferred slot**

Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port.

---

**threshold { threshold_type}**

Restores the system defaults for the selected threshold. The possible threshold types are:

- **high-activity**: High port activity threshold settings
- **monitoring**: Threshold monitoring configuration settings
- **rx-utilization**: Receive port utilization threshold settings
- **tx-utilization**: Transmit port utilization threshold settings

---

**Usage**

Restores port-level parameters to their default values.

---

**Example**

```
default preferred slot
```
**description**

Defines descriptive text that provides useful information about the port.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
description text
no description
```

- **no**
  Erases the port’s defined description from the configuration file.

- **text**
  `text` must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

**Usage**

Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters.

**Example**

```
description samplePortDescriptiveText

description "This is a sample description"
```
end

Exits the ATM Port configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
```
end
```

Usage
Change the mode back to the Exec mode.
exit

Exits the ATM Port configuration mode and returns to the global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the Global configuration mode.
line-timing

This command enables the SPIO to recover transmit timing source via line attached to the selected port. By default, line-timing is not enabled.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] line-timing

no
Disables line-timing as the source for the transmit clock.

Usage
The port must be enabled (no shutdown) to enable recovery of timing source via the line. As well, the card’s slot number must be entered in the recover line# command of the BITS port configuration mode.

Example
Disable timing clock recovery on this port.

no line-timing
preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the LC in slot 17 while ports 5 through 8 are “preferred” on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

preferred slot slot#
[ default | no ] preferred slot

default
Default: non-revertive operation.

no
Disables revertive, or auto-recovery, operation for the port.

slot#
Identifies the physical slot in the chassis where the preferred line card is installed.

Usage
This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically. Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

Example

preferred slot 17
**pvc**

This command creates a Permanent Virtual Connection (PVC), including the definition of the associated Virtual Path Identifiers (VPI) and Virtual Connection Identifiers (VCI) for the PVC. By defining a PVC, this command enters into PVC configuration mode. The ATM port supports a maximum of 256 PVC definitions.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] pvc vpi vpi# vci vci#
```

- **no**
  Deletes the PVC’s entry from the configuration.

- **vpi vpi#**
  VPI identifies a unique path to a destination point in the ATM portion of the network. The VPI and the VCI combine to create the PVC between the MS and the destination point. **vpi#** must be an integer, 0 to 255.

- **vci vci#**
  VCI identifies a unique virtual circuit within the associated VPI. **vci#** must be an integer, 0 to 65535.

**Usage**
Creates a virtual circuit between two specific points that the carrier will use repeatedly.

**Example**
Define a PVC with VPI 2 and VCI 353.

```
pvc vpi 2 vci 353
```
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the no keyword enables the port.

Product: SGSN
Privilege: Security Administrator, Administrator

Syntax:

```
shutdown
no shutdown
```

```
no
```

Enables the port’s administrative state. When omitted the card is shutdown (removed from service).

Usage:

Shut down a port prior to re-cabling and/or other maintenance activities. This command with the no keyword is required to bring a port into service.

Example:

```
shutdown
no shutdown
```
snmp trap link-status

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

snmp trap link-status

no snmp trap link-status

no
Disables the sending of traps for link-status changes.

Usage
Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

Example

snmp trap link-status

no snmp trap link-status
threshold high-activity

Configures the port’s high and low activity thresholds.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
threshold high-activity high_threshold [ clear low_threshold]
```

**high_threshold**
Default: 50
Sets the threshold for the highest percentage of port activity that must be met or exceeded, within the polling interval, to generate an alert or alarm.

**clear low_threshold**
Default: 50
Sets the threshold for the lowest percentage level of port activity that must be met to generate and send a clear alarm. If port activity does not drop to or below this threshold then the alarm is maintained.

_Important:_ This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port ≥ High Threshold
- **Clear condition:** Actual percent utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

Example
The following command configures a high port utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
threshold high-activity
threshold monitoring

Enables thresholding for port-level values.

Product
All

Privilege
Security Administrator, Administrator

Syntax

threshold monitoring

no threshold monitoring

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference. The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until a the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 12. Thresholding Reporting Mechanisms by Model
This command enables thresholding for port-level values. Refer to the sections covering `threshold high-activity`, `threshold rx-utilization`, and `threshold tx-utilization` commands in this chapter for information on configuring these values. In addition, refer to the `threshold poll` command in the `Global Configuration Mode Commands` chapter of this reference for information on configuring the polling interval over which these values are monitored.
threshold rx-utilization

Configures thresholds for receive-port utilization.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
threshold rx-utilization  high_thresh  [ clear  low_thresh ]
```

- **high_thresh**
  
  Default: 80
  
  The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  The percentage can be configured to any integer value between 0 and 100.

- **clear low_thresh**
  
  Allows the configuration of the low threshold.
  
  Default: 80
  
  The low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
  
  The percentage can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for received data ≥ High Threshold
- **Clear condition:** Actual percent utilization of a port for received data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**
The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```
threshold tx-utilization

Configures thresholds for transmit port utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
threshold tx-utilization high_thresh [ clear low_thresh ]
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **high_thresh** | Default: 80  
The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.  
The percentage can be configured to any integer value between 0 and 100. |
| **clear low_thresh** | Allows the configuration of the low threshold.  
Default: 80  
The low threshold transmit port utilization percentage that maintains a previously generated alarm condition.  
If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.  
The percentage can be configured to any integer value between 0 and 100. |

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data ≥ High Threshold  
- **Clear condition:** Actual percent utilization of a port for transmit data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**
The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```
Chapter 21
Bandwidth Policy Configuration Mode Commands

The Bandwidth Policy Configuration Mode is used to create and manage ACS bandwidth policies.

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

Returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to change to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.
flow limit-for-bandwidth

This command configures the ACS Bandwidth-Policy Flow Limit-for-bandwidth configuration.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
flow limit-for-bandwidth id bandwidth_id group-id group_id

no flow limit-for-bandwidth id bandwidth_id
```

**Usage**
Use this command to configure the ACS Bandwidth-Policy Flow Limit-for-bandwidth configuration.

**Example**
The following command configures the flow limit-for-bandwidth configuration with bandwidth policy ID test123 and group ID 123:

```
flow limit-for-bandwidth id test123 group-id 123
```
group-id

This command configures the ACS Bandwidth-Policy Group ID.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
group-id group_id direction { downlink | uplink } peak-data-rate bps peak-burst-size bytes violate-action { discard | lower-ip-precedence } [ committed-data-rate bps committed-burst-size bytes [ exceed-action { discard | lower-ip-precedence } ] ]
```

- **default**
  Configures default settings for the specified group ID.

- **no**
  Removes configuration for the specified group ID.

- **group_id**
  Specifies the group ID.
  *group_id* must be an integer from 1 through 65535.

- **direction { downlink | uplink }**
  Specifies the direction for which bandwidth will be controlled.

- **peak-data-rate bps**
  Specifies peak data rate in bits per second.
  *bps* must be an integer from 1 through 4294967295.
  Default: 0

- **peak-burst-size bytes**
  Specifies peak burst size in bytes.
  *bytes* must be an integer from 1 through 4294967295.
  Default: 0

- **violate-action { discard | lower-ip-precedence }**
  Specifies the action to be taken if Peak Data Rate is surpassed.
  - **discard** Specifies to discard the packet
  - **lower-ip-precedence** Specifies to lower IP precedence of the packet
 specifies the committed Data Rate in bits per second. This can also be used to specify GBR in NCQoS (without the exceed-action).

\[ bps \] must be an integer from 1 through 4294967295.
Default: 0

**committed-burst-size bytes**

Specifies the committed burst size in bytes.

\[ bytes \] must be an integer from 1 through 4294967295.
Default: 0

**exceed-action { discard | lower-ip-precedence }**

Specifies the action to be taken if Committed Data Rate is surpassed.

**discard**: Specifies to discard the packet

**lower-ip-precedence**: Specifies to lower IP precedence of the packet

**Usage**

Use this command to configure the ACS Bandwidth-Policy Group ID.

**Example**

The following command configures group ID of 111 to control bandwidth for the downlink direction specifying peak data rate of 10000 bits per second and peak burst size of 10000 bytes while specifying the action to be taken on violation as discard:

```
group-id 111 direction downlink peak-data-rate 10000 peak-burst-size 10000 violate-action discard
```
Chapter 22
BGP Address-Family (IPv4/IPv6) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (IPv4/IPv6) Configuration Mode is used to configure the IPv4 and IPv6 address family information.
Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**
Return to the context configuration mode.
neighbor

This command configures IPv4/IPv6 Address Family for BGP routers that interconnect to non-broadcast networks.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

neighbor ip_address {activate|advertisement-interval adv_time | default-originate [route-map map_name] | distribute-list dist_list {in | out} | ebgp-multihop [max-hop number] | filter-list filt_list {in | out} | max-prefix max_num [threshold thresh_percent] [warning-only] | remote-as AS_num | remove-private-AS | route-map map_name {in | out} | shutdown | timers {{connect-interval conn_time} | [keepalive-interval keep_time Holdtime-interval hold_time]} | update-source ip_address | weight value}

no
Delete the specified parameter from the router configuration.

activate
Enable the exchange of routes with this neighbor.

advertisement-interval adv_time
The minimum interval, in seconds, between sending BGP routing updates. 
adv_time must be an integer from 0 through 600.
Default: 30

default-originate [route-map map_name]
Originates default routes to this neighbor 
route-map map_name: Specifies the route-map that contains the criteria to originate default routes. 
map_name must be the name of an existing route-map in the current context.

distribute-list dist_list {in | out}
Filter updates to and from this neighbor based on a route access list. 
Default: No filtering is performed. 
dist_list: The name or number of an existing route-access-list. 
in: Indicates that incoming advertised routes should be filtered. 
out: Indicates that outgoing advertised routes should be filtered.

ebgp-multihop [max-hop number]
Allow EBGP neighbors not on directly connected networks. 
max-hop number: The maximum number of hops allowed to reach a neighbor. number must be an integer from 1 through 255. 
Default hop count: 255
filter-list filt_list {in | out}
Establish BGP filters based on an AS path access list.
   filt_list: The name of an existing AS path access list.
   in: Indicates that incoming advertised routes will be filtered.
   out: Indicates that outgoing advertised routes will be filtered.

max-prefix max_num [threshold thresh_percent] [warning-only]
The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.
   max_num: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
   Default: No maximum prefix limit.
   threshold thresh_percent: A percentage value which specifies that when the BGP table is the specified percentage full from this peer warnings are sent to the neighbor. thresh_percent must be an integer from 1 through 100.
   warning-only: This keyword specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset.

remote-as AS_num
Specify the AS number of the BGP neighbor.
   AS_num: The neighbor’s autonomous system number. must be an integer from 1 through 65535.

remove-private-AS
Remove the private AS number from outbound updates.
   Default: Do not remove the private AS number.

route-map map_name {in | out}
Apply a route map to the neighbor.
   map_name: Specifies the route-map apply. map_name must be the name of an existing route-map in the current context.
   in: Indicates that the route map applies to incoming advertisements.
   out: Indicates that the route map applies to outgoing advertisements.

shutdown
Administratively shut down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

timers {{connect-interval conn_time] | [keepalive-interval keep_time Holdtime-interval hold_time]}}
BGP timers for the specified neighbor.
   connect-interval conn_time: Specifies the connect timer in seconds. conn_time must be an integer from 0 through 65535. The default is 60 seconds.
   keepalive-interval keep_time: The frequency, in seconds, at which the current BGP router sends keepalive messages to its neighbor. keep_time must be an integer from 0 through 65535. The default is 30 seconds.
   Holdtime-interval hold_time: The interval, in seconds, the router waits for a keepalive message before declaring a neighbor dead. hold_time must be an integer from 0 through 65535. The default is 90 seconds.
**update-source** *ip_address*

use this keyword to bind the specified IP address to the bgp socket that is used to communicate to the peer.  
*ip_address* is an IPv4 address in dotted decimal notation.  
In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the tcp connection does not go down until there is no route for the loopback address in the peering router.

**weight** *value*

This command sets the default weight for routes from this neighbor.  
*value*: This must be an integer from 0 through 65535.  
Default: 0

---

**Usage**

Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

---

**Important**: A remote AS number must be specified for a neighbor before other parameters can be configured.

---

**Example**

The following command specifies that the neighbor at the IP address 192.168.100.25 has an AS number of 2000:

```
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of 27 hops away:

```
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes

```
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to 100:

```
neighbor 192.168.100.25 weight 100
```
network

This command configures and specifies a network to announce via BGP.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
network ip_address/mask [ route-map map_name ]
no network ip_address/mask [ route-map map_name ]
```

**no**
Delete the specified network from the configuration for the BGP router.

**ip_address/mask**
Specifies the IP address and netmask bits for the network to announce via BGP. *ip_address* is a network IP address (in dotted-decimal notation) and *mask* is the number of subnet bits, representing a subnet mask in shorthand. These must be entered in the IPv4 dotted-decimal notation/subnet bits format.

**route-map map_name**
Filter routes through the specified route map before announcing the network. *map_name* specifies the name of the route-map to use and must be specified as a string of 1 through 79 alphanumeric characters.

**Usage**
Use this command to specify a network to announce via BGP.

**Example**
The following command announces the network 192.168.0.0 with a netmask of 16 via BGP:

```
  network 192.168.0.0/16
```

The following command removes the network from the BGP router configuration:

```
  no network 192.168.0.0/16
```
**redistribute**

This command redistributes routes into BGP. This means that any routes from another protocol are redistributed to BGP neighbors using the BGP protocol.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] redistribute {connected | ospf | rip | static} [route-map map_name]
```

- **no**
  Remove the specified redistribution parameters from the BGP router configuration.

- **connected**
  Specifies that connected routes will be redistributed.

- **ospf**
  Specifies that OSPF routes will be redistributed

- **rip**
  Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

- **static**
  Specifies that static routes will be redistributed.

- **route-map map_name**
  Filter routes through the specified route map before redistribution.
  `map_name` specifies the name of the route-map to use and must be specified as a string of 1 through 79 alphanumeric characters

**Usage**

Use this command to specify what routes this BGP router should redistribute into BGP.

**Example**

The following command redistributes OSPF routes after filtering them through the route map named Map1:

```
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router’s configuration:

```
no redistribute ospf route-map Map1
```
Chapter 23
BGP Address-Family (VPNv4) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (VPNv4) Configuration Mode is used to configure the VPNv4 address family information.
**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the context configuration mode.
neighbor

This command configures VPNv4 address family on BGP routers that interconnect to non-broadcast networks and enables the exchange of routing information with a peer router (neighbor).

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
[no] neighbor ip_address {activate| remote-as AS_num | send-community {both | extended | standard} }
```

- **no**
  Delete the specified parameter from the router configuration.

- **ip_address**
  Specifies the IP address of the peer router (neighbor).

- **activate**
  Enable the exchange of routing information with this neighbor.

- **remote-as AS_num**
  Specify the AS number of the BGP neighbor.
  
  \[ AS_num \]
  The neighbor’s autonomous system number. must be an integer from 1 through 65535.

- **send-community extended**
  This keyword sends the extended community attributes to a peer router (neighbor).

Usage

Use this command to enable the exchange of routing information with a peer router. The chassis supports a maximum of 64 peers per context.

**Important:** A remote AS number must be specified for a neighbor before other parameters can be configured.

Example

The following command specifies that the neighbor at the IP address 192.168.100.25 has an AS number of 2000:

```
neighbor 192.168.100.25 remote-as 2000
```
Chapter 24
BGP Address-Family (VPNv4) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (VPNv4) Configuration Mode is used to configure the VPNv4 address family information.
Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
**exit**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the context configuration mode.
neighbor

This command configures IPv4/IPv6 Address Family for BGP routers that interconnect to non-broadcast networks.

Product  
HA

Privilege  
Security Administrator, Administrator

Syntax

[no] neighbor ip_address {activate|advertisement-interval adv_time | default-originate [route-map map_name] | distribute-list dist_list {in | out} | ebgp-multihop [max-hop number] | filter-list filt_list {in | out} | max-prefix max_num [threshold thresh_percent] [warning-only] | remote-as AS_num | remove-private-AS | route-map map_name {in | out} | shutdown | timers [{[connect-interval conn_time]} | [keepalive-interval keep_time Holdtime-interval hold_time]}]} | update-source ip_address | weight value

---

no

Delete the specified parameter from the router configuration.

---

activate

Enable the exchange of routes with this neighbor.

---

advertisement-interval adv_time

The minimum interval, in seconds, between sending BGP routing updates.  
adv_time must be an integer from 0 through 600.  
Default: 30

---

default-originate [route-map map_name]

Originate default routes to this neighbor  
route-map map_name: Specifies the route-map that contains the criteria to originate default routes.  
map_name must be the name of an existing route-map in the current context.

---

distribute-list dist_list {in | out}

Filter updates to and from this neighbor based on a route access list.  
Default: No filtering is performed.  
dist_list: The name or number of an existing route-access-list.  
in: Indicates that incoming advertised routes should be filtered.  
out: Indicates that outgoing advertised routes should be filtered.

---

egbp-multihop [max-hop number]

Allow EBGP neighbors not on directly connected networks.  
max-hop number: The maximum number of hops allowed to reach a neighbor. number must be an integer from 1 through 255.  
Default hop count: 255
filter-list \texttt{filt_list} \{\texttt{in} \mid \texttt{out}\}

Establish BGP filters based on an AS path access list
\texttt{filt_list}: The name of an existing AS path access list.
\texttt{in}: Indicates that incoming advertised routes will be filtered.
\texttt{out}: Indicates that outgoing advertised routes will be filtered.

\textbf{max-prefix} \texttt{max_num} [\texttt{threshold} \texttt{thresh_percent}] [\texttt{warning-only}]

The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.
\texttt{max_num}: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
Default: No maximum prefix limit.
\texttt{threshold} \texttt{thresh_percent}: A percentage value which specifies that when the BGP table is the specified percentage full from this peer warnings are sent to the neighbor. \texttt{thresh_percent} must be an integer from 1 through 100.
\texttt{warning-only}: This keyword specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset.

\textbf{remote-as} \texttt{AS_num}

Specify the AS number of the BGP neighbor.
\texttt{AS_num}: The neighbor’s autonomous system number. must be an integer from 1 through 65535.

\textbf{remove-private-AS}

Remove the private AS number from outbound updates.
Default: Do not remove the private AS number.

\textbf{route-map} \texttt{map_name} \{\texttt{in} \mid \texttt{out}\}

Apply a route map to the neighbor.
\texttt{map_name}: Specifies the route-map apply. \texttt{map_name} must be the name of an existing route-map in the current context.
\texttt{in}: Indicates that the route map applies to incoming advertisements.
\texttt{out}: Indicates that the route map applies to outgoing advertisements.

\textbf{shutdown}

Administratively shut down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

\textbf{timers} \{[\texttt{connect-interval} \texttt{conn_time}] \mid [\texttt{keepalive-interval} \texttt{keep_time} \texttt{Holdtime-interval} \texttt{hold_time}]\}

BGP timers for the specified neighbor.
\texttt{connect-interval} \texttt{conn_time}: Specifies the connect timer in seconds. \texttt{conn_time} must be an integer from 0 through 65535. The default is 60 seconds.
\texttt{keepalive-interval} \texttt{keep_time}: The frequency, in seconds, at which the current BGP router sends keepalive messages to its neighbor. \texttt{keep_time} must be an integer from 0 through 65535. The default is 30 seconds.
\texttt{Holdtime-interval} \texttt{hold_time}: The interval, in seconds, the router waits for a keepalive message before declaring a neighbor dead. \texttt{hold_time} must be an integer from 0 through 65535. The default is 90 seconds.
use this keyword to bind the specified IP address to the bgp socket that is used to communicate to the peer. 

ip_address is an IPv4 address in dotted decimal notation.

In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the tcp connection does not go down until there is no route for the loopback address in the peering router.

weight value

This command sets the default weight for routes from this neighbor.

value: This must be an integer from 0 through 65535.

Default: 0

Usage

Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

Important: A remote AS number must be specified for a neighbor before other parameters can be configured.

Example

The following command specifies that the neighbor at the IP address 192.168.100.25 has an AS number of 2000:

```plaintext
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of 27 hops away:

```plaintext
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes

```plaintext
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to 100:

```plaintext
neighbor 192.168.100.25 weight 100
```
redistribute

This command redistributes routes into BGP. This means that any routes from another protocol are redistributed to BGP neighbors using the BGP protocol.

Product
HA

Privilege
Security Administrator, Administrator

Syntax


Usage
Use this command to specify what routes this BGP router should redistribute into BGP.

Example
The following command redistributes OSPF routes after filtering them through the route map named Map1:

```
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router’s configuration:

```
no redistribute ospf route-map Map1
```
Chapter 25
BITS Port Configuration Mode Commands

The Building Integrated Timing Supply (BITS) port configuration mode provides the commands to configure the BITS ports on the SPIO and optionally to configure the transmit timing source.

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

Restores the port’s default speed and communication mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
default { mode | preferred slot }
```

### mode
Sets the default for the ports framing mode. The default is no mode configuration.

### preferred slot
Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port.

Usage
Restores port-level parameters to their default values.

Example
default preferred slot
description

Defines descriptive text that provides useful information about the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

description text

no description

Usage
Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters.

text

text must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Example

description samplePortDescriptiveText
description "This is a sample description"
end

Exits the BITS port configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the BITS port configuration mode and returns to the Global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the Global configuration mode.
mode

Configures the framing mode for the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

mode { e1 | t1 } framing type

  e1 | t1
  e1 selects the SDH E1 framing mode.
  t1 selects the SONET T1 framing mode.

  framing type
  basic selects the Frame Alignment Signal (FAS) used with E1.
  crcmf selects the Multiframe with CRC (FAS+CRC) used with E1.
  esf selects the extended superframe format used with T1.
  sf selects the superframe format (D4) used with T1.

Usage
Set the ports framing mode parameters.

Example
Configure the port to support E1 with crcmf framing.

mode e1 framing crcmf
preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. There are only two SPIO, one in slot 24 and the other in slot 25.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

preferred slot  slot#
[ default | no ] preferred slot

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: non-revertive operation.</td>
</tr>
</tbody>
</table>

| no |
| Disables revertive, or auto-recovery, operation for the port. |

| slot# |
| Identifies the physical slot in the chassis where the SPIO is installed. |

Usage

This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically. Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch command to return service to the original port.

Example

preferred slot 25
recover

Configure line-timing so the SPIO recovers the transmit timing source from an external source via one of the line cards in the chassis. The recovered clock is then distributed for use to all line cards in the chassis.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

recover { line1 slot# | line2 slot# }  

no recover { line1 | line2 }

no
Deletes the identified line-timing source definition from the configuration.

line1 slot#
Sets first priority for line-timing clock recovered from the line card in the specified slot.
slot#: a number between 1 and 48.

line2 slot#
Sets second priority for line-timing clock recovered from the line card in the specified slot.
slot#: a number between 1 and 48. Can not be the same slot number entered for line1.

Usage
Define which line-timing source has priority.

Example
Configure the line card in slot 19 as the preferred line-timing source.

recover line1 19
**shutdown**

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the `no` keyword enables the port and BITS-timing as a transmit timing source.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
shutdown

no shutdown
```

Enables the port’s administrative state. When omitted the card is shutdown (removed from service).

**Usage**
Shut down a port prior to re-cabling and/or other maintenance activities.
This command with the `no` keyword is required to bring a port into service.

**Example**

```
shutdown

no shutdown
```
**snmp trap link-status**

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
snmp trap link-status
no snmp trap link-status
```

- **no**
  Disables the sending of traps for link-status changes.

**Usage**
Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

**Example**

```
snmp trap link-status
no snmp trap link-status
```
Chapter 26
BMSC Profile Configuration Mode Commands

The BMSC Profile Configuration Mode is used to configure Broadcast Multicast Service Center profiles for Multimedia Broadcast Multicast Service (MBMS) applications. The mode is accessed by entering the bmsc-profile command from the Context Configuration Mode.

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
Returns the CLI prompt to the Exec mode.

**Syntax**

```plaintext
end
```

**Usage**

Change the mode back to the Exec mode.

**Example**

```plaintext
end
```
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the previous or parent mode.

Example

```
exit
```
gmb diameter dictionary

Specifies the Diameter dictionary for the Gmb interface in BM-SC profile of MBMS user service.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
כמות diameter dictionary { custom1 | custom10 | custom2 | custom3 | custom4 | custom5 | custom6 | custom7 | custom8 | custom9 | standard }
default gmb diameter dictionary
```

- **custom1 ... custom10**
  Custom-defined Diameter dictionary. Specific to customer requirement.

- **standard**
  Default: Enabled
  Specifies the standard Gmb Diameter dictionary conforming to 3GPP TS 29.061 (Rel. 7).

- **default**
  Sets the Diameter dictionary to standard.

**Usage**
Use this command to select the Gmb Diameter dictionary in BM-SC profile of MBMS user service.

**Example**
The following command sets the Gmb Diameter dictionary to TS 29.061 (Rel. 7) specific:

```plaintext
gmb diameter dictionary standard
```
gmb diameter endpoint

Specifies the Diameter endpoint name for Gmb interface in BM-SC profile of MBMS user service.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gmb diameter endpoint endpoint_name
```

```
no gmb diameter endpoint
```

```
no
```

Removes the previously configured Diameter endpoint name for Gmb interface in BM-SC profile of MBMS user service.

```
endpoint_name
```

Specifies the Diameter endpoint name for Gmb interface. This must be present in all Diameter messages and is the endpoint that originates the Diameter message.

`endpoint_name` must be an alpha and/or numeric string of length between 1 to 63 characters.

Usage
Use this command to create a Gmb Diameter endpoint for BM-SC profile.

Example
The following command creates a Diameter endpoint named `test1` in BM-SC profile of MBMS user service:

```
gmb diameter endpoint test1
```
gmb diameter peer-select

Specifies the peer ids of BM-SC Diameter primary and secondary host in BM-SC profile for MBMS user service.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gmb diameter peer-select peer peer_name [ realm realm_name ] [ secondary-peer sec_peer_name [ realm sec.realm_name ] ]
gmb diameter peer-select no
```

peer peer_name
Specifies the primary diameter host id for BM-SC in this BM-SC profile for MBMS user service. This is a unique name that is specified for the primary peer.
peer_name must be an alpha and/or numeric string of from 1 through 127 characters and it allows punctuation marks.

realm realm_name
Specifies the realm or domain for Gmb diameter peer. The realm may typically be a company or service name.
realm_name must be an alpha and/or numeric string of from 1 to 127 characters and allows punctuation marks.

secondary-peer sec_peer_name
Specifies a back-up host that is used for fail-over processing. When the route-table does not find an AVAILABLE route the secondary host performs a fail-over processing.
sec_peer_name must be an alpha and/or numeric string of from 1 through 127 characters and it allows punctuation marks.

realm sec.realm_name
Specifies the realm or domain for Gmb diameter secondary host. The realm may typically be a company or service name.
sec.realm_name must be an alpha and/or numeric string of from 1 to 127 characters and allows punctuation marks.

Usage
Use this command to select a BM-SC Diameter peer and realm in this BM-SC profile for MBMS user service.
Example
The following command selects a Gmb Diameter peer named test1 and a realm of companyx.
```
gmb diameter peer-select peer test1 realm companyx
```
gmb user-data

This command configures the parameters in this BM-SC profile for user data of MBMS user service.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gmb user-data { mode-preference { multicast | unicast } | unicast-self-address self_ip_address }
default gmb user-data mode-preference
no gmb user-data unicast-self-address
```

no
Removes the configured self address of GGSN for unicast in BM-SC profile for user data of MBMS user service.

default
Sets the user data mode to unicast in BM-SC profile for user data of MBMS user service.

```
mode-preference { multicast | unicast }
```
Default: unicast
Specifies the preferred mode of GGSN for receiving MBMS user service data.
multicast: specifies the preferred mode as multicast for MBMS user service.

```
Important: Note that this multicast keyword is not supported in this release.
```

unicast: specifies the preferred mode as unicast for MBMS user service.

```
unicast-self-address self_ip_address
```
Specifies the GGSN’s IP address for BM-SC to use as outer destination address for the IP-in-IP tunnel to send multicast data if configured preferred data mode is unicast.

self_ip_address must be the IPv4 address in dotted decimal notation.
This command must be configured if GGSN's user-data mode-preference is Unicast.

Usage
Use this command to configure user data mode and other parameters in BM-SC profile for user data of MBMS user service.

GGSN can receive multicast data from BM-SC in one of two modes - Multicast or Unicast. In Unicast mode, BM-SC tunnels the multicast data to the GGSN in an IP-in-IP tunnel instead of direct multicast. This
command with mode-preference keyword configures the GGSN's preferred mode for receiving multicast data.

**Important:** Both GGSN and BM-SC must support the Unicast mode of multicast data transfer. If any of GGSN or BM-SC doesn't support Multicast mode, BM-SC will transfer multicast data using Unicast mode only.

Use unicast-self-address keyword to configure GGSN’s IP address which the BM-SC should use as the outer destination address for the IP-in-IP tunnel to send multicast data if the selected user data mode to receive multicast data is Unicast (i.e. either of GGSN or BM-SC doesn't support Multicast mode of data transfer).

**Example**
The following command sets the MBMS data transfer mode to unicast:

```plaintext
default gmb user-data mode-preference
```
Chapter 27
Border Gateway Protocol Configuration Mode Commands

The Border Gateway Protocol (BGP) Configuration Mode is used to configure properties for BGP-4 routing.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          router bgp asn
            BGP Configuration Mode
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
address-family ipv4

Configures the IPv4 Address Family information for the specified BGP AS number. Optionally it also enables the VRF routing information, if specified.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax
address-family ipv4 [ vrf vrf_name]

[no] address-family ipv4 vrf vrf_name

- **no**
  This keyword removes the configured IPv4 address family VRF mode for specific BGP AS number.

- **vrf vrf_name**
  This optional keyword enables the exchange of VRF routing information. When this keyword is specified with this command then the address family mode changed to VRF address family mode for specific BGP AS number.

**Important:** The route distinguisher id must be configured for this VRF name through `route-distinguisher` command in BGP VRF Configuration mode, before using this keyword.

Usage
Use this command to configure the IPv4 BGP address family configuration parameters for BGP router and optionally enables the exchange of VRF routing information. This command is also used to switch the command mode to enter the BGP Address Family Configuration Mode.

Use of `address-family ipv4` command switch the command mode to `BGP Address Family Configuration Mode` and prompt will be changed to the following:

```
[context_name>@host_name(config-bgp-af-v4)#
```

Use of `address-family ipv4 vrf vrf_name` command switch the command mode to BGP Address Family Configuration Mode and prompt will be changed to the following:

```
[context_name>@host_name(config-bgp-af-vrf)#
```

Example
Use following command to enter the IPv4 BGP Address-Family configuration mode:

```
address-family ipv4
```
Use following command to enter the IPv4 VRF BGP Address-Family configuration mode for exchange of VRF routing information from VRF route_vrf1:

```
address-family ipv4 vrf route_vrf1
```
address-family ipv6

Configures the IPv6 Address Family information for the specified BGP AS number.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
address-family ipv6
```

**Usage**

Use this command to configure the IPv6 BGP address family configuration parameters for BGP router. This command is also used to switch the command mode to enter the BGP Address Family Configuration Mode. Use of `address-family ipv6` command switches the command mode to BGP Address Family Configuration Mode and prompt will be changed to the following:

```
[context_name>]host_name(config-bgp-af-v6)#
```

**Example**

Use the following command to enter the IPv6 BGP Address-Family configuration mode:

```
address-family ipv6
```
address-family vpnv4

Configures the VPNv4 Address Family information for the specified BGP AS number.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax
address-family vpnv4

Usage
Use this command to configure the VPNv4 address family configuration parameters for BGP router. This command is also used to switch the command mode to enter the BGP Address Family Configuration Mode. Use of address-family vpnv4 command switches the command mode to BGP Address Family Configuration Mode and prompt will be changed to the following:

[context_name>]host_name(config-bgp-af-vpnv4)#

Example
Use the following command to enter the BGP Address-Family configuration mode for VPNv4 address parameters:

address-family vpnv4
distance

Define the administrative distance for routes. The administrative distance is the default priority for a specific route or type route.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

distance { admin distance prefix prefix_addr [ route-access-list list_name ] | bgp external ebgp_dist internal ibgp_dist local local_dist }

no distance { admin distance prefix prefix_addr [ route-access-list list_name ] | bgp [ external ebgp_dist internal ibgp_dist local local_dist ] }

Usage

Use this command to set the administrative distance for specific routes to values that you specify. These values are only applied to the current router.

Example
Use the following command to set the administrative distance to 100 for all routes that have an IP prefix of 192.168.0.0 with a netmask of 16 and are specified in a remote access list named racl1:

distance admin 100 prefix 192.168.0.0/16 route-access-list racl1
**end**

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

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

`end`

**Usage**

Return to the Exec mode.
enforce-first-as

Enforce the first Autonomous System (AS) for Exterior Border Gateway Protocol (EBGP) routes. As stated in RFC1930; “An AS is a connected group of one or more Internet Protocol prefixes run by one or more network operators which has a single and clearly defined routing policy.”

Product
HA

Privilege
Security Administrator, Administrator

Syntax

    enforce-first-as

Usage
Use this command to enforce the use of the first AS for EBGP routes.

Example
Use the following command to enable this functionality:

    enforce-first-as
exit

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

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the context configuration mode.
ip vrf

This command adds a preconfigured IP VRF context instance to the BGP ASN and configures the BGP attributes and related parameters to the VRF. This command also switches the command mode to BGP VRF Configuration mode.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

[no] ip vrf vrf_name

no
Removes an associated IP VRF from specified BGP AS number and other configured parameters.

vrf_name
Specifies the IP VRF context configured in the Context configuration mode and to be associated with a BGP AS number.

vrf_name must be a string from 1 to 79 identifying an existing instance.

Usage
Use this command to associate the specified IP VRF context instance to the BGP AS number and configures the BGP attributes and related parameters to the VRF. This command also switches the command mode to BGP VRF Configuration mode.

This command switches the command mode to **BGP IP VRF Configuration Mode** and prompt will be changed to the following:

[context_name>]host_name(config-bgp-vrf)#

Example
Use the following command associates the pre-defined VRF context instance *router_mpls* to this BGP AS number:

**ip vrf router_mpls**
neighbor

This command configures BGP routers that interconnect to non-broadcast networks. Note that a remote AS number must be specified for a neighbor before other parameters can be configured.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

[no] neighbor ip_address {activate|advertisement-interval adv_time | default-originate [route-map map_name] | distribute-list dist_list (in | out) | ebgp-multihop [max-hop number] | filter-list filt_list (in | out) | max-prefix max_num [threshold thresh_percent] [warning-only] | remote-as AS_num | remove-private-AS | route-map map_name (in | out) | shutdown | timers {[connect-interval conn_time] | [keepalive-interval keep_time | Holdtime-interval hold_time]} | update-source ip_address | weight value]

no
Delete the specified parameter from the router configuration.

activate
Enable the exchange of routes with this neighbor.

advertisement-interval adv_time
The minimum interval, in seconds, between sending BGP routing updates.
Default: 30
adv_time must be an integer from 0 through 600.

default-originate [route-map map_name]
Originate default routes to this neighbor
route-map map_name: Specifies the route-map that contains the criteria to originate default routes.
map_name must be the name of an existing route-map in the current context.

distribute-list dist_list (in | out)
Filter updates to and from this neighbor based on a route access list.
Default: No filtering is performed.
dist_list: The name or number of an existing route-access-list.
in: Indicates that incoming advertised routes should be filtered.
out: Indicates that outgoing advertised routes should be filtered.

ebgp-multihop [max-hop number]
Allow EBGP neighbors not on directly connected networks.
Default hop count: 255
max-hop number: The maximum number of hops allowed to reach a neighbor. number must be an integer from 1 through 255.
**Border Gateway Protocol Configuration Mode Commands**

- **filter-list filt_list {in | out}**
  Establish BGP filters based on an AS path access list.
  - *filt_list*: The name of an existing AS path access list.
  - *in*: Indicates that incoming advertised routes will be filtered.
  - *out*: Indicates that outgoing advertised routes will be filtered.

- **max-prefix max_num [threshold thresh_percent] [warning-only]**
  The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.
  - *max_num*: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
  - *threshold thresh_percent*: A percentage value which specifies that when the BGP table is the specified percentage full from this peer warnings are sent to the neighbor. *thresh_percent* must be an integer from 1 through 100.
  - *warning-only*: This keyword specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset.

- **remote-as AS_num**
  Specify the AS number of the BGP neighbor.
  - *AS_num*: The neighbor’s autonomous system number. must be an integer from 1 through 65535.

- **remove-private-AS**
  Remove the private AS number from outbound updates.
  Default: Do not remove the private AS number.

- **route-map map_name {in | out}**
  Apply a route map to the neighbor.
  - *map_name*: Specifies the route-map apply. *map_name* must be the name of an existing route-map in the current context.
  - *in*: Indicates that the route map applies to incoming advertisements.
  - *out*: Indicates that the route map applies to outgoing advertisements.

- **shutdown**
  Administratively shut down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

- **timers {{connect-interval conn_time} | [keepalive-interval keep_time Holdtime-interval hold_time]}}**
  BGP timers for the specified neighbor.
  - *connect-interval conn_time*: Specifies the connect timer in seconds. *conn_time* must be an integer from 0 through 65535. The default is 60 seconds.
  - *keepalive-interval keep_time*: The frequency, in seconds, at which the current BGP router sends keepalive messages to its neighbor. *keep_time* must be an integer from 0 through 65535. The default is 30 seconds.
  - *Holdtime-interval hold_time*: The interval, in seconds, the router waits for a keepalive message before declaring a neighbor dead. *hold_time* must be an integer from 0 through 65535. The default is 90 seconds.
**neighbor**

**update-source ip_address**

use this keyword to bind the specified IP address to the bgp socket that is used to communicate to the peer.  
*ip_address* is an IPv4 address in dotted decimal notation.  
In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the tcp connection does not go down until there is no route for the loopback address in the peering router.

**weight value**

This command sets the default weight for routes from this neighbor.  
Default: 0  
value: This must be an integer from 0 through 65535.

**Usage**

Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

**Example**

The following command specifies that the neighbor at the IP address 192.168.100.25 has an AS number of 2000:

```plaintext
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of 27 hops away:

```plaintext
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes:

```plaintext
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to 100:

```plaintext
neighbor 192.168.100.25 weight 100
```
network

Specify a network to announce via BGP

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
network ip_address/mask [route-map map_name]
no network ip_address/mask [route-map map_name]
```

**no**
Delete the specified network from the configuration for the BGP router.

**ip_address/mask**
Specifies the IP address and netmask bits for the network to announce via BGP. *ip_address* is a network IP address (in dotted-decimal notation) and *mask* is the number of subnet bits, representing a subnet mask in shorthand. These must be entered in the dotted-decimal notation/subnet bits format (1.1.1.1/24).

**route-map map_name**
Filter routes through the specified route map before announcing the network. *map_name* specifies the name of the route-map to use and must be specified as a string of 1 through 79 alphanumeric characters.

Usage
Use this command to specify a network to announce via BGP.

Example
The following command announces the network 192.168.0.0 with a netmask of 16 via BGP:
```
network 192.168.0.0/16
```
The following command removes the network from the BGP router configuration:
```
no network 192.168.0.0/16
```
**redistribute**

This command redistributes routes into BGP. This means that any routes from another protocol are redistributed to BGP neighbors using the BGP protocol.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redistribute { connected | ospf | rip | static } [ route-map map_name ]
```

- `no`
  Remove the specified redistribution parameters from the BGP router configuration.

- `connected`
  Specifies that connected routes will be redistributed.

- `ospf`
  Specifies that OSPF routes will be redistributed.

- `rip`
  Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

- `static`
  Specifies that static routes will be redistributed.

- `route-map map_name`
  Filter routes through the specified route map before redistribution. `map_name` specifies the name of the route-map to use and must be specified as a string of 1 through 79 alphanumeric characters.

**Usage**

Use this command to specify what routes this BGP router should redistribute into BGP.

**Example**
The following command redistributes OSPF routes after filtering them through the route map named Map1:

```
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router’s configuration:

```
no redistribute ospf route-map Map1
```
router-id

Override the configured router identifier (peers will reset).

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
router-id ip_address
no router-id [ip_address]
```

no
Remove the specified router ID from the router’s configuration and use the default router ID.

```
ip_address
```
The IP address to use as the BGP router ID. `ip_address` must be an IPv4 address in dotted decimal notation (###.###.###.###).

Usage
Use this command to configure a specific router ID that overrides the default.

Example
The following command sets the router ID to 192.168.100.25:
```
router-id 192.168.100.25
```
scan-time

Configure background scanner interval. The background scanner scans routers for next hop validation.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
scan-time time
no scan-time
```

```
no
Remove the user specified scan time from the router’s configuration. The scan time is reset to the default value.
```

```
time
Default: 60
The amount of time, in seconds, to wait between background scans to determine next-hop validity. time must be an integer from 5 through 60.
```

Usage
Use this command to set the background scanner interval for the BGP router.

Example
The following command sets the background scanner interval to 30 seconds:
```
scan-time 30
```
**timers**

This command configures BGP routing timers.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
timers bgp Keepalive-interval interval Holdtime-interval time [ Min-peer-holdtime-interval ] time
no timers bgp
```

**no**

Remove the user specified timer values from the router’s configuration. The timer values are reset to the default values.

**Keepalive-interval interval**

Default: 30

The interval, in seconds, to wait between sending keepalive packets. Must be an integer from 0 through 65535.

**Holdtime-interval time**

Default: 90

The interval, in seconds, after which the neighbor is considered dead if keepalive messages are not received. Must be an integer from 0 through 65535.

**Min-peer-holdtime-interval time**

Default: 0

The interval, in seconds, that is the minimum acceptable hold time from a neighbor. Must be an integer from 0 through 65535. The default is 0 so that there is no restriction on the hold time received in an OPEN message from the peer.

**Usage**

Use this command to configure the how long to wait between sending keepalive packets and how long to wait for a keepalive before considering a neighbor dead.

**Example**

The following command sets the keepalive interval to 2 minutes and the holdtime interval to 3 minutes:

```
timers bgp Keepalive-interval 120 Holdtime-interval 180 Min-peer-holdtime-interval 0
```
Chapter 28
Border Gateway Protocol IP VRF Configuration Mode Commands

The Border Gateway Protocol (BGP) IP VRF Configuration Mode is used to configure properties for BGP-4 routing.
**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
route-distinguisher

This command assigns a route distinguisher (RD) for the VRF. The route distinguisher value must be a unique value on the router for each VRF.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
route-distinguisher {as_value | ip_address} rd_value
```

```
as_value
The ASN value is a 16-bit autonomous-system (AS) number from 0 through 65535.

ip_address }
ip_address is an 32 bit IP address in IPv4 dotted decimal notation.

rd_value }
rd_value is an unique route distinguisher identifier and must be an integer between 0 through 4294967295.
```

Usage
Use this command to assign a router distinguisher (RD) for the IP VRF. The combination of AS number/IP address and RD value must be unique for every VRF configured. The RD is added to the beginning of the pool addresses to change them into globally unique VPN-IPv4 prefixes.

If the RD is not configured for a VRF, user cannot enter into the BGP Address-Family mode for that VRF to configure the neighbors or other related BGP commands.

An RD assigined to a VRF cannot be changed until the existing VRF is deleted or removed and reconfigured.

Example
The following command assigns a router distinguisher 12345 to VRF with AS number 300:

```
route-distinguisher 300 12345
```

The following command assigns a router distinguisher 12345 to VRF with IP address 1.5.3.4:

```
route-distinguisher 1.5.3.4 12345
```
route-target

This command adds a list of import and/or export route target extended communities to the VRF.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

route-target {both | import | export} {as_value | ip_address} rt_value

<table>
<thead>
<tr>
<th>both</th>
</tr>
</thead>
</table>
| This keyword creates list of import and export route targets for the VRF with same parameters. The list contains AS number or IP address along with RT value.

import

This keyword creates list of import route targets for the VRF with same parameters. The list contains AS number or IP address along with RT value.

export

This keyword creates list of import route targets for the VRF with same parameters. The list contains AS number or IP address along with RT value.

<table>
<thead>
<tr>
<th>as_value</th>
</tr>
</thead>
</table>
| The ASN value is a 16-bit autonomous-system (AS) number from 0 through 65535.

<table>
<thead>
<tr>
<th>ip_address</th>
</tr>
</thead>
</table>
| ip_address is an 32 bit IP address in IPv4 dotted decimal notation.

<table>
<thead>
<tr>
<th>rt_value</th>
</tr>
</thead>
</table>
| rt_value is an unique route target identifier and must be an integer between 0 through 4294967295.

Usage

Use this command to create the list of export and/or import route target extended communities for VRF. It specifies the a target VPN extended community.

A maximm of 5 route targets can be defined with this command up to release 9.0.

A maximm of 10 route targets can be defined with this command from release 10.0 onward.

**Important:** This command must be executed for each route target extended communities.

Example


The following command creates an export list of route target extended community 12345 for VRF with AS number 300:

```
route-target export 300 12345
```

The following command creates an export list of route target extended community 12345 for VRF with IP address 192.168.1.2:

```
route-target export 192.168.1.2 12345
```
Chapter 29
Bulk Statistics File Configuration Mode Commands

This section describes a bulk statistic “file” under which to group the bulk statistic configuration. The Bulk Statistics File Configuration mode supports the configuration of “files” used for organizing bulk statistics schema, delivery options, and receiver information.

Because multiple “files” can be configured, this functionality provides greater flexibility in that it allows you to configure different schemas to go to different receivers. To configure a bulk statistics file, enter the following command:

```
Important: Use of bulk statistics “files” is optional. However system logically assigns “file 1” to the standard configuration. Therefore, if you wish to configure bulk statistics “files” at a later time, “file 1” can be used.
```

```
Caution: If the Web Element Manager application is used to collect and process (XML parsing, graphing, etc.) bulk statistics data, “file 1” is used by the Web Element Manager’s default bulk statistics collection information and schemas. To avoid errors in processing by the Web Element Manager, do not configure “file 1” via the CLI. However, it is possible to configure files 1 through 4 using the system’s CLI, regardless of whether or not the Web Element Manager is configured as a receiver. In this case, the bulk statistics data is written to the server but not processed by the Web Element Manager application.
```

```
Important: The commands in this configuration mode are identical to the same commands in the “Bulk Statistics Configuration Mode Commands” chapter.
```
Chapter 30
Bulk Statistics Configuration Mode Commands

The Bulk Statistics Configuration Mode is used to manage the system statistics options for collection and delivery as well as for the format of data delivered to remote nodes.

Refer to the Common Syntax Options section in this chapter for information about formatting bulk statistics output.

**Important:** Unless otherwise indicated, all statistics are counters. For statistics with the Int32 data type, the roll-over to zero limit is 4,294,967,295. For statistics with the Int64 data type, the roll-over to zero limit is 18,446,744,073,709,551,615.

```
Exec Mode
  configure
  Global Configuration Mode
    bulkstats mode
    Bulkstats Configuration Mode
```
Common Syntax Options

The following defines common syntax block options. These options appear in similar commands and are detailed here for easy reference.

Schema Format String Syntax

The schema format string is used to define the structure of generated bulk statistics data. The string may contain static text, dynamic content, and bulk statistic variables, or any combination.

Static text includes any ASCII characters that are of a fixed value. Static text may also include control characters by using escape character sequences.

Escape character shortcuts are supported are “\n” for new line and “\t” for tab.

Variables within the format string must be enclosed within “%”, for example “%var%”. The actual variables supported are command-dependent and are described in the Statistics and Counters Reference.
Common Statistics

For a list of the statistics that are common to all schema, refer to the Statistics and Counters Reference.
apn schema

This command configures APN bulk statistics schema.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```plaintext
apn schema schema_name format format_string

no apn schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema name.
  ```plaintext
  schema_name
  ```
  Must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  Specifies the schema format.
  ```plaintext
  format format_string
  ```
  Must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for APN bulk statistics collection. Multiple APN schemas can be created to further categorize APN-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple APN schemas, re-issue the apn schema command using a different schema name.

Example

The following command creates a schema called apnlstats1 that records the number of sessions currently facilitated by the APN:

```plaintext
apn schema apnlstats1 format "@sess-curr@"
```
asngw schema

This command configures ASN-GW bulk statistics schema.

**Product**
ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
asngw schemas schema_name format format_string

no asngw schemas schema_name
```

*no*
Removes the specified schema.

*schema_name*
Specifies the schema name.
*schema_name* must be an alpha and/or numeric string of 1 through 31 characters in length.

*format format_string*
Specifies the schema format.
*format_string* must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important**: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for ASN-GW bulk statistics collection. Multiple ASN-GW service schemas can be created to further categorize ASN-GW service bulk statistics. All of the schemas are processed at each collection interval. To create multiple ASN-GW service schemas, re-issue the `asngw schema` command using a different schema name.

**Example**

To create an ASN-GW schema called `asngw_statistics` that specifies a schema format of:
- VPN context name: `vpnname`
- VPN Context Identifier: `vpnid`
- ASN-GW Service name: `servname`
- ASN-GW Service identifier: `servid`
- Peer IP address: `peeripaddr`
Use the following command:

```
asngw schema asngw_statistics format "VPN name: %vpnname\nVPN ID: %vpid\nASN-GW Service Name: %servername\nASN-GW Service Identifier: %servid\nPeer IP Address: %peeripaddr"
```
**bcmcs schema**

This command configures BCMCS bulk statistics schema.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
bcmcs schema schema_name format format_string
no bcmcs schema schema_name
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
|Removes the specified schema.

<table>
<thead>
<tr>
<th>schema_name</th>
</tr>
</thead>
</table>
|Specifies the schema name. 
|schema_name must be an alpha and/or numeric string of 1 through 31 characters in length.

<table>
<thead>
<tr>
<th>format format_string</th>
</tr>
</thead>
</table>
|Specifies the schema format. 
|format_string must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for BCMCS bulk statistics collection. Multiple BCMCS schemas can be created to further categorize BCMCS-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple BCMCS schemas, re-issue the bcmcs schema command using a different schema name.

**Example**

The following command creates a schema named bcmcs1stats1 that records the number of sessions currently facilitated by BCMCS:

```
bcmcs schema bcmcs1stats1 format "@sess-curr@"
```
card schema

This command configures card bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Syntax

card schema schema_name format format_string

no card schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema name.

format format_string
Specifies the schema format.
format_string must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for card bulk statistics collection. Multiple card schemas can be created to categorize card-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple card schemas, re-issue the card schema command using a different schema name.

Important: Not supported on all platforms

Example
The following command creates a schema called card1stats1 that records the number of processes for all installed cards:

card schema card1stats1 format "%slot%-%numproc%"

To create a card-level schema called cardresourcestats that specifies a schema format of:
Chassis slot number: slot
Available Memory: memtotal Memory Used (%): memused
Available CPU (%): cpuidle
Use the following command:

```
   card schema cardresourcestats format "Chassis slot number: %slot%
   Available Memory: %memtotal%
   Memory Used (%): %memused%
   Available CPU (%): %cpuidle%"
```
context schema

This command configures Firewall bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ccontext schema

\textit{schema\_name}

Specifies the schema name.

\textit{schema\_name} must be an alpha and/or numeric string of 1 through 31 characters in length.

\textit{format\_string}

Specifies the schema format.

\textit{format\_string} must be an alpha and/or numeric string of 1 through 3600 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see \textit{Schema Format String Syntax} section.

\textbf{Important:} For the complete list of the statistics that are supported for this schema, refer to the \textit{Statistics and Counters Reference}.

Usage

Use this command to define schemas for Context bulk statistics collection. Multiple context schemas can be created to categorize context statistics. All of the schemas are processed at each collection interval. To create multiple context schemas, re-issue the context schema command using a different schema name.

Example

To create a context schema called \textit{sfw\_context\_stats1} that specifies a schema format of:

- Total packets received by firewall: \textit{sfw-total-rxpackets}
- Total packets sent by firewall: \textit{sfw-total-txpackets}
- Total ICMP packets discarded by firewall: \textit{fw-icmp-discardpackets}

Use the following command:
context schema sfw_context_stats1 format "Packets received Rx: %sfw-total-rxpackets%nPackets Sent Tx: %sfw-total-txpackets%nICMP Packets discarded: %fw-icmp-discardpackets\""
cscf schema

This command configures CSCF bulk statistics schema.

Product
SCM

Privilege
Security Administrator, Administrator

Syntax

```
cscf schema schema_name format format_string
no cscf schema schema_name
```

```
no
Removes the specified schema.

schema_name
Specifies the schema name.
`schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

format format_string
Specifies the schema format.
`format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see `Schema Format String Syntax` section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the `Statistics and Counters Reference`.

Usage

Use this command to define schemas for CSCF bulk statistics collection. Multiple CSCF-service schemas can be created to categorize CSCF-service bulk statistics. All of the schemas are processed at each collection interval. To create multiple CSCF-service schemas, re-issue the `cscf schema` command using a different schema name.

Example

To create a CSCF schema called `cscf_statistics` that specifies a schema format of:

- Call attempts received: `callattrx`
- Call attempts transmitted: `callatttx`
- Call successes received: `callsuccrx`
- Call successes transmitted: `callsucctx`
- Call failures received: `callfailrx`
• Call failures transmitted: `callfailtx`

Use the following command:

```
cscf schema cscf_statistics format "Call Attempts Rx: %callattrx%nCall Attempts Tx: %callatttx%nCall Successes Rx: %callsuccrx%nCall Successes Tx: %callsuccctx%nCall Failures Rx: %callfailrx%nCall Failures Tx: %callfailtx"
```
**dcca schema**

This command configures Diameter Credit Control Application (DCCA) bulk statistics schema. This command is available only in StarOS 9.0 and later releases.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dcca schema schema_name format format_string
no dcca schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema name.
  `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  Specifies the schema format.
  `format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for DCCA bulk statistics collection.
default

Restores the system default for the option specified.

Product
All

Privilege
Security Administrator, Administrator

Syntax

default { limit | receiver mode | remotefileformat | sample-interval | transfer-interval }

limit
Restores the memory utilization limit system default: 1000 kilobytes.

receiver mode
Restores the behavior for sending files to the receivers to the default value.
Default: secondary-on-failure

remotefile format
Restores the format of remote bulkstats file names to the default value.
Default: “%date%-%time%”

sample-interval
Restores the system default for the local polling interval for statistic sampling.
Default: 15 minutes

transfer-interval
Restores the system default for the time between transfer of data files to receivers.
Default: 480 minutes

Usage
Restore the default values when troubleshooting the system. Setting values to the system defaults places them in well known states as starting points for monitoring for problems.

Example
default limit
default transfer-interval
dpca schema

This command configures Diameter Policy Control Application (DPCA) bulk statistics schema. This command is available only in StarOS 9.0 and later releases.

Product
All

Privilege
Security Administrator, Administrator

Syntax

dpca schema schema_name format format_string

no dpca schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema name.
schema_name must be an alpha and/or numeric string of 1 through 31 characters in length.

format format_string
Specifies the schema format.
format_string must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for DPCA bulk statistics collection.
**ecs schema**

This command configures Enhanced Charging Service (ECS) bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ecs schema schema_name format format_string
no ecs schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema name.
  *schema_name* must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  Specifies the schema format.
  *format_string* must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for ECS bulk statistics collection. Multiple ECS schemas can be created to categorize ECS bulk statistics. All of the schemas are processed at each collection interval. To create multiple ECS schemas, re-issue the `ecs schema` command using a different schema name.
egtpc schema

Configures the enhanced GTP-C statistics schema for naming conventions of data files.

Product
P-GW, S-GW

Privilege
Administrator

Syntax

```bash
egtpc schema schema_name format format_string

no egtpc schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema name.
  - `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  - Specifies the schema format.
  - `format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see the `Schema Format String Syntax` section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the `Statistics and Counters Reference`.

Usage

Use this command to define schemas for enhanced GTP-C bulk statistics collection. Multiple eGTP-C service schemas can be created to categorize eGTP-C service bulk statistics. All of the schemas are processed at each collection interval. To create multiple eGTP-C service schemas, re-issue the `egtpc schema` command using a different schema name.

Example

For an eGTP-C-level schema called `egtpcservicestats` that specifies a schema format of:

```
Tunnel - Create Session Request Sent: tun-sent-creseess
Tunnel - Create Session Request Received: tun-recev-creseess
```

Use the following command:

```bash
egtpc schema egtpcservicestats format "Number of GTP Tunnel Requests Sent: %tun-sent-creseess\nNumber of GTP Tunnel Requests Received: %tun-recev-creseess\n"
```
**end**

Exits the bulk statistics configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the bulk statistics configuration mode and returns to the global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the global configuration mode.
**fa schema**

This command configures Foreign Agent (FA) bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
fa schema schema_name format format_string
no fa schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema name.
  *schema_name* must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  Specifies the schema format.
  *format_string* must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see the **Schema Format String Syntax** section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for FA bulk statistics collection. Multiple FA service schemas can be created to categorize FA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple FA service schemas, re-issue the **fa schema** command using a different schema name.

**Example**

To create a FA-level schema named *faservicestats* that separates the *date, time, and vpnname* by tabs, enter the following command:

```
fa schema faservicestats format @date@\t@time@\t@vpnname@
```

The schema format appears as follows:

date  time  vpnname
file

Enters the Bulk Statistics File Configuration mode which supports the configuration of “files” used for grouping bulk statistic configuration information.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] file number

- **no**
  Removes a previously configured bulk statistic file.

- **number**
  Specifies the a number for the bulkstatistics file. This number is how the file is recognized by the system. *number* must be an integer value from 1 to 4.

Usage

Bulk statistics “files” are used to group bulk statistic schema, delivery options, and receiver configuration. Because multiple “files” can be configured, this functionality provides greater flexibility in that it allows you to configure different schemas to go to different receivers. A Maximum of 4 files can be assigned for bulk statistics collection.

Executing this command allows you to enter the Bulk Statistics File Configuration Mode. This mode supports all of the commands from the Bulk Statistics Configuration mode except **limit**, **local-directory**, **sample-interval**, and **transfer-interval** (these commands are configured globally for all “files”).

**Important:** Use of bulk statistics “files” is optional. If you do not wish to configure bulk statistic “files”, you can perform a standard configuration using the commands in the Bulk Statistic Configuration Mode. Note, however, that the system logically assigns “file 1” to the standard configuration. Therefore, if you wish to configure bulk statistics “files” at a later time, “file 1” will already be used.

**Caution:** If the Web Element Manager application is used to collect and process (XML parsing, graphing, etc.) bulk statistics data, “file 1” is used by the Web Element Manager’s default bulk statistics collection information and schemas. To avoid errors in processing by the Web Element Manager, do not configure "file 1" via the CLI. However, it is possible to configure files 1 through 4 using the system’s CLI, regardless of whether or not the Web Element Manager is configured as a receiver. In this case, the bulk statistics data is written to the server but not processed by the Web Element Manager application.

Example
The following command creates a bulk statistics file numbered 2 and enter the Bulk Statistics File Configuration Mode:
file 2
**footer**

Configures the footer string placed in the end of the generated bulk statistics data files.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
footer format format_string
no footer format

no
```

Clears the footer format string which results in the default file footer being used in generated data files.

```plaintext
format format_string
```

Default: “” (an empty footer)

Specifies the footer format string for use in generated data files. *format_string* must be from 1 to 2047 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described in the [Schema Format String Syntax](#) section.

The following variables are supported:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>The date that the collection file was created in YYYYMMDD format where YYYY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>host</td>
<td>The system hostname that created the file</td>
<td>String</td>
</tr>
<tr>
<td>ipaddr</td>
<td>The default management (local context) IP address in ###.###.###.### format. An empty string is inserted if no address is available.</td>
<td>String</td>
</tr>
<tr>
<td>sysuptime</td>
<td>The uptime (in seconds) of the system that created the file.</td>
<td>32-bit signed</td>
</tr>
<tr>
<td>time</td>
<td>The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.</td>
<td>String</td>
</tr>
</tbody>
</table>

**Usage**

Define a unique footer in data files which allows for easy identification of which system generated the data file or any other useful information. The use of the variables is suggested so as to allow for a uniform footer across all systems. The hostname variable should be used to identify the source of the data in the footer and all remaining items can be formatted consistently across all chassis.
Example
Following command can be used to define different header formats:

```
footer format northStreet
footer format "Created on: %date%-%time% by %host%"
no footer format
```
gather-on-standby

This command controls whether or not statistics are gathered when a system is in the standby state.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no | default ] gather-on-standby

no
Do not gather bulk statistics when the system is in the standby state.

default
Reset this command to its default action of gathering bulk statistics when the system is in the standby state.

Usage
Use this command to configure a system to either gather or not gather statistics when the system is in the standby state. This is useful for HA or GGSN systems configured for Interchassis Session Recovery. See the System Administration Guide for more details on this feature.
If a chassis transitions to standby state and it has accumulated but not yet transferred bulk statistics data, the previously accumulated data is transferred at the first opportunity, but no additional statistics gathering takes place.

Example
The following command disables gathering statistics when the system is in the standby state:

    no gather-on-standby

The following command enables the gathering of statistics when the system is in the standby state:

    gather-on-standby
gprs schema

This command configures GPRS bulk statistics schema.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gprs schema schema_name format format_string

no gprs schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema name.
  `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  Specifies the schema format.
  `format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the [*Statistics and Counters Reference*](#).
gtpc schema

This command configures GPRS Tunneling Protocol-Control (GTPC) message statistics schema.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpc schema gtpc_schema_name format gtpc_schema_format
no gtpc schema gtpc_schema_name
```

- **no**
  Removes the specified schema.

- **gtpc_schema_name**
  Specifies the schema name.
  **gtpc_schema_name** must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format gtpc_schema_format**
  Specifies the schema format.
  **gtpc_schema_format** must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for GTPC bulk statistics collection. Multiple GTPC schemas can be created to categorize GTPC bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTPC schemas, re-issue the **gtpc schema** command using a different schema name.

Example

To create a GTPC-level schema named **gtpc_stats** that specifies a schema format of:

- **Context Name:** vpnname
- **GGSN Service Name:** servname
- **Total PDP Contexts Processed:** setup-total

Use the following command:

```
gtpc schema gtpc_stats format "Context Name: %vpnname%nGGSN Service Name: %servname%nTotal PDP Contexts Processed: %setup-total%n"
```
**gtpp schema**

This command configures GPRS Tunneling Protocol-Prime (GTPP) statistics schema.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp schema gtpp_schema_name format gtpp_schema_format

no gtpp schema gtpp_schema_name
```

- `no`
  Removes the specified schema.

- `gtpp_schema_name`
  Specifies the schema name.
  `gtpp_schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- `format gtpp_schema_format`
  Specifies the schema format.
  `gtpp_schema_format` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax section](#).

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for GTPP bulk statistics collection. Multiple GTPP schemas can be created to categorize GTPP bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTPP schemas, re-issue the `gtpp schema` command using a different schema name.

**Example**

To create a GTPP schema named `gtpp_statistics` that specifies a schema format of:

- **Time:** time
- **Total Redirection Requests Received:** `redir-rcvd`

Use the following command:

```
gtpp schema gtpp_statistics format "Time: %time%\tTotal Redirection Requests Received: %redir-rcvd%\n"
```
ha schema

This command configures Home Agent (HA) bulk statistics schema.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

ha schema <schema_name> format <format_string>

no ha schema <schema_name>

no
Removes the specified schema.

<schema_name>
Specifies the schema name.
<schema_name> must be an alpha and/or numeric string of 1 through 31 characters in length.

format <format_string>
Specifies the schema format.
<format_string> must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for HA bulk statistics collection. Multiple HA service schemas can be created to categorize HA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple HA service schemas, re-issue the ha schema command using a different schema name.

Example
For an HA schema named haservicestats that specifies a schema format of:
Number of HA authentication failures: reply-hauthfail
Number of Mobile Node authentication failures: reply-mauthfail
Use the following command:

    ha schema haservicestats format "Number of HA authentication failures: %reply-hauthfail%nNumber of Mobile Node authentication failures: %reply-mauthfail%n"
**header**

Configures the header string placed in the beginning of the generated bulk statistics data files.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
header format format_string
no header format
```

no

Clears the header format string which results in the default file header being used in generated data files.

```plaintext
format format_string
```

Default: "" (an empty header)

Specifies the header format string for use in generated data files. `format_string` must be from 1 to 2047 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described in the [Schema Format String Syntax](#) section.

The following variables are supported:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>The UTC date that the collection file was created in YYYYMMDD format where YYY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>date3</td>
<td>The UTC date that the collection file was created in YYMMDD format where YY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>host</td>
<td>The system hostname that created the file</td>
<td>String</td>
</tr>
<tr>
<td>ipaddr</td>
<td>The default management (local context) IP address in ###.###.###.### format. An empty string is inserted if no address is available.</td>
<td>String</td>
</tr>
<tr>
<td>sysuptime</td>
<td>The uptime (in seconds) of the system that created the file.</td>
<td>32-bit signed</td>
</tr>
<tr>
<td>time</td>
<td>The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.</td>
<td>String</td>
</tr>
</tbody>
</table>

**Usage**

Define a unique header in data files which allows for easy identification of which system generated the data file or any other useful information.
The use of the variables is suggested so as to allow for a uniform header across all systems. The hostname variable should be used to identify the source of the data in the header and all remaining items can be formatted consistently across all chassis.

Example
Following command can be used to define different header formats:

```
header format northStreet
header format "Created on: %date%-%time% by %host%"
no header format
```
ippool schema

This command configures IP pool bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ippool schema schema_name format format_string

no ippool schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema name.
schema_name must be an alpha and/or numeric string of 1 through 31 characters in length.

format format_string
Specifies the schema format.
f format_string must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for IP pool bulk statistics collection. Multiple IP pool schemas can be created to further IP pool bulk statistics. All of the schemas are processed at each collection interval. To create multiple IP pool schemas, re-issue the ippool schema command using a different schema name.

Example

To create an IP pool schema named ippoolstats that specifies a schema format of:
Number of IP addresses on hold: hold
Number of free IP addresses: free
Use the following command:

ippool schema ippoolstats format "Number of IP addresses on hold: $hold\nNumber of free IP addresses: $free\n"
ipsg schema

This command configures IP Services Gateway (IPSG) bulk statistics schema.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

ipsg schema schema_name format format_string

no ipsg schema schema_name

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define the schemas used for IPSG bulk statistics collection. Multiple IPSG schemas can be created to categorize IPSG bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the ipsg schema command using a different schema name.

Example
To create an IPSG schema named ipsgstats that specifies a schema format of:
Context name: vpnname
Service name: servname
Total responses sent: total-rsp-sent

Use the following command:

    ipsg schema ipsgstats format "Context name: $vpnname$\nService name: $servname$\nTotal responses sent: $total-rsp-sent$\n"
**lac schema**

This command configures LAC bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
lac schemaschema_nameformatformat_string
```

no lac schemaschema_name

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema name. `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  Specifies the schema format. `format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [TSchema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**
Use this command to define schemas for LAC bulk statistics collection. Multiple LAC schemas can be created to categorize LAC bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `lac schema` command using a different schema name.

**Example**
The following command creates a schema called lac1stats1 that records the number of active subscriber sessions and the number of sessions that failed or were disconnected due to the maximum tunnel limit being reached:

```
lac schema lac1stats1 format "@sess-curactive@-@sess-maxtunnel@"
```

To create a schema called lacresourcestats that specifies a schema format of:
Number of Successful Session Connections: sess-successful
Number of Session Attempts That Failed: sess-failed
Number of Sessions Currently Active: sess-curative
Use the following command:
lac schema lacresourcestats format "Number of Successful Session Connections: %sess-successful%
Number of Session Attempts That Failed: %sess-failed%
Number of Sessions Currently Active: %sess-curative%"
**limit**

Configures the maximum amount of system memory bulk statistics may utilize.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
limit kilobytes
```

- `kilobytes`: Specifies the maximum amount of memory, in kilobytes, that may be used for bulk statistics. `kilobytes` must be a value in the range from 1 to 32000.

**Usage**

Adjust bulk statics memory usage when considering the sampling interval adjustments.
The system is shipped from the factory with the limit set to 1000.

⚠️ **Caution:** Bulk statistics are stored in Random Access Memory (RAM) on the SMC. In the event of power loss or system failure, the statistics will be lost. If the maximum storage limit has been reached before the system's configured transfer-interval is reached, the oldest information stored in the collection will be overwritten.

**Example**

```
limit 2048
```
**Ima schema**

Configures the Local Mobility Anchor (LMA) statistics schema for naming conventions of data files.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
lma schema schema_name format format_string
no lma schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema name.
  - `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  - Specifies the schema format.
  - `format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for LMA bulk statistics collection. Multiple LMA service schemas can be created to categorize LMA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple LMA service schemas, re-issue the `lma schema` command using a different schema name.

**Example**

For an LMA-level schema called `lmaservicestats` that specifies a schema format of:

- `Binding Update Received: bindupd`
- `Binding Update Received - Denied: bindupd-denied`

Use the following command:

```
lma schema lmaservicestats format "Number of Binding Updates Received: %bindupd\nNumber of Binding Updates Received and Denied: %bindupd-denied\n"
```
local-directory

Sets the local directory for storing bulkstats collection files

Product
All

Privilege
Security Administrator, Administrator

Syntax

local-directory <pathname>
nolocal-directory

no
Delete the setting for local-directory.

pathname
The local path of the directory in which to store bulkstats collection files. This must be an alpha and/or numeric string of 1 to 127 characters. Pathnames are case sensitive.

Usage
Use this command to designate a directory on a local file system in which collection files with bulkstats information are stored. The directory specified must already exist. Use the Exec Mode command mkdir to create a directory.

Example
To specify that bulkstats collection files are stored in the local directory /flash/bulkstats, enter the following command:

    local-directory /flash/bulkstats
**mag schema**

Configures the Mobile Access Gateway (MAG) statistics schema for naming conventions of data files.

**Product**
HSGW, S-GW

**Privilege**
Administrator

**Syntax**

```
mag schemascalenameformatformat_string

no mag schemascalename
```

**no**
Removes the specified schema from MAG bulk statistics generation.

```
schema_name
```

Specifies the name to use to refer to the schema and associated format string.

*schema_name* must be an alpha and/or numeric string of 1 through 31 characters in length.

```
format format_string
```

Specifies the schema format.

*format_string* must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for MAG bulk statistics collection. Multiple MAG service schemas can be created to categorize MAG service bulk statistics. All of the schemas are processed at each collection interval. To create multiple MAG service schemas, re-issue the `mag schema` command using a different schema name.

**Example**
For a MAG-level schema called `magservicestats` that specifies a schema format of:

- Binding Update Sent: bindupd
- Binding Acknowledgement Received: bindack

Use the following command:

```
mag schema magservicestats format "Number of Binding Updates Sent: %bindupd\nNumber of Binding Acknowledgements Received: %bindack\n"
```
mipv6ha schema

This command configures MIPv6 HA bulk statistics schema.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
mipv6ha schema schema_name format format_string

no mipv6ha schema schema_name
```

**no**
Removes the specified schema.

`schema_name`
Specifies the schema name.
- `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

`format format_string`
Specifies the schema format.
- `format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see *Schema Format String Syntax* section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**
Use this command to define schemas for MIPv6 HA bulk statistics collection. Multiple MIPv6 HA bulk statistics schemas can be created to categorize MIPv6 HA bulk statistics. All of the schemas are processed at each collection interval. To create multiple MIPv6 HA service schemas, re-issue the `mipv6ha schema` command using a different schema name.

**Example**
The following command creates a schema called `mipv6haservicestats` that records the number of authorization attempt failures due to access rejects from AAA:

```plaintext
mipv6ha schema mipv6haservicestats format "%aaa-actauthfail%"
```
nat-realm schema

This command creates and configures Network Address Translation (NAT) realm statistics schema.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
nat-realm schema schema_name format format_string
no nat-realm schema schema_name
```

- **schema_name**
  Specifies the NAT realm bulk statistics schema name.
  *schema_name* must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  Specifies the schema format.
  *format_string* must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for NAT Realm bulk statistics collection. Multiple NAT realm schemas can be created to further categorize NAT realm level bulk statistics. All of the schemas are processed at each collection interval. To create multiple NAT Realm schemas, re-issue the `nat-realm schema` command using a different schema name.

**Example**

The following command creates a NAT realm schema with the VPN name, realm name, and flows information:

```plaintext
nat-realm schema realm1 format "@vpname@ @realmname@ @nat-rlm-flows@
```
**pdif schema**

This command configures PDIF bulk statistics schema.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
pdif schema schema_name format format_string
```

```
no pdif schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema name.
  - `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  - Specifies the schema format.
  - `format_string` must be an alpha and/or numeric string of 1 through 3600 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for PDIF bulk statistics collection. Multiple PDIF schemas can be created to categorize PDIF bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `pdif schema` command using a different schema name.

**Example**

The following command creates a schema called `pdifschema1` for the category current active ipv4 sessions:

```
pdif schema pdifschema1 format `sess-curactipv4`
```
port schema

This command configures port bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Syntax

port schema schema_name format format_string

no port schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema name. 
schema_name must be an alpha and/or numeric string of 1 through 31 characters in length.

format format_string
Specifies the schema format. 
format_string must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for port bulk statistics collection. Multiple port schemas can be created to categorize port-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple port schemas, re-issue the port schema command using a different schema name.

Important: The card variable in the Port schema is not supported on all platforms

Example
To create a port-level schema named portstats1 that separates the card/port, bcast_inpackets, and bcast-outpackets variables by hyphens ("-"), enter the following command:

port schema portstats1 format "%card%/ %port% - %bcast_inpackets% - %bcast_outpackets%"
**ppp schema**

This command configures point-to-point protocol bulk statistics schema.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
ppp schema schema_name format format_string
no ppp schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema name.
  - `schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **format format_string**
  - Specifies the schema format.
  - `format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for point-to-point protocol bulk statistics collection. Multiple PPP-service schemas can be created to categorize PPP-service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PPP-service schemas, re-issue the `ppp schema` command using a different schema name.

**Example**

To create a ppp-level schema named `pppstats` that specifies a schema format of:

CHAP:

FAP:

Use the following command:
```plaintext
```
radius schema

This command configures RADIUS bulk statistics schema.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
radius schema schema_name format format_string
no radius schema schema_name
```

**no**
Removes the specified schema.

**schema_name**
Specifies the schema name.
```
schema_name must be an alpha and/or numeric string of 1 through 31 characters in length and is case sensitive.
```

**format format_string**
Specifies the schema format.
```
format_string must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.
```

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for RADIUS bulk statistics collection. Multiple RADIUS schemas can be created to categorize RADIUS bulk statistics. All of the schemas are processed at each collection interval. To create multiple RADIUS schemas, re-issue the radius schema command using a different schema name.

Example
To create a RADIUS schema named radius_statistics that specifies a schema format of:

- Server: ipaddr
- Authentication Requests Sent: auth-req-sent
- Accounting Requests Sent: acc-req-sent

Use the following command:

```
radius schema radius_statistics format Server: ipaddr Authentication Requests Sent: auth-req-sent Accounting Requests Sent: acc-req-sent
```
radius schema radius_statistics format "Server: %ipaddr%
Authentication Requests Sent: %auth-req-sent%
Accounting Requests Sent: %acc-req-sent%"
receiver

Configures host system to receive bulkstats information through TFTP transfer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
receiver { mode { redundant | secondary-on-failure } | ip_address { primary | secondary } [ mechanism { { { ftp | sftp } login user_name [ encrypted ] password pwd } | tftp } ] }
```

```
no receiver ip_address
```

```
no
```

Removes the receiver specified from the list of receivers where data files are sent.

```
mode { redundant | secondary-on-failure }
```

Determines how bulkstats are delivered to the primary and secondary receivers.

Default: `secondary-on-failure`  
`redundant`: Files are transferred to both the primary and secondary receivers. If either transfer isn't possible, the file is transferred when possible. The system continues to hold in memory as much data as possible until the data has been successfully transferred to both receivers. Data is only discarded if the in-memory data reaches the configured limit. Refer to the `limit` command.  
`secondary-on-failure`: Files are transferred to the secondary receiver if the primary receiver fails. In-memory data is erased once the data is transferred to either the primary or secondary receiver. This is the default behavior.

```
ip_address
```

Specifies the IP address of the receiver of interest. `ip_address` must be specified using the standard IPv4 dotted decimal notation.

```
primary | secondary
```

Primary and secondary are used to indicate the order in which receivers are connected. The secondary is used when the primary is unreachable.  
`primary`: indicates the receiver is the primary receiver of data.  
`secondary`: indicates the receiver is the secondary receiver of data.

```
mechanism { { { ftp | sftp } login user_name [ encrypted ] password pwd } | tftp } }
```

Specifies the method by which data is transferred to the receiver.  
`ftp login user_name [ encrypted ] password pwd`: the FTP protocol shall be used for data file transfer. `user_name` specifies the user to provide for remote system secure logins and must be an alpha and/or numeric string of 1 through 31 characters in length. The password to use for remote system
authentification is specified as \( pwd \) and must be from 1 to 31 alpha and/or numeric characters or 1 to 64 alpha and/or numeric characters if the \texttt{encrypted} keyword is also specified.

\texttt{sftp login user\_name [ encrypted] password \( pwd \)}: the SFTP protocol shall be used for data file transfer. \texttt{user\_name} specifies the user to provide for remote system secure logins and must be an alpha and/or numeric string of 1 through 31 characters in length. The password to use for remote system authentication is specified as \( pwd \) and must be from 1 to 31 alpha and/or numeric characters or 1 to 64 alpha and/or numeric characters if the \texttt{encrypted} keyword is also specified.

\texttt{tftp}: the TFTP protocol is to be used to transfer files. The \texttt{encrypted} keyword is intended only for use by the system while saving configuration scripts. The system displays the \texttt{encrypted} keyword in the configuration file as a flag that the variable following the \texttt{password} keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**Usage**

Use TFTP methods to reduce transfer times if excessive system resources are being used across the network for transfer of data.

FTP transfer method allows for login which then provides system logging within the enabled FTP logs. The initial connection is attempted to the primary. If the primary is unreachable for any reason the secondary is used. If the secondary is also unreachable the system retries after a delay period where it again attempts to connect to the primary followed by the secondary as necessary.

---

**Important:** For redundant receivers, configuration changes to the receivers are applied to all existing and all subsequent data sets pending transfer. If no receiver is configured, bulk statistics will be collected and stored on the system until the maximum amount of memory is used; they will not be transferred to the receiver(s). When the storage limit has been reached the oldest information is overwritten. When a receiver is configured for the primary and secondary target, this command will use both receivers as default if no receiver is specified.

---

**Example**

```
receiver 1.2.3.4 primary mechanism tftp receiver 1.2.3.5 secondary no receiver 1.2.3.4
```
remotefile

Configures the naming convention with support for multiple file format to multiple receivers when storing the data files on the remote receiver/s.

Product
All

Privilege
Security Administrator, Administrator

Syntax

remotefile format format_string [ both-receivers | primary-receiver | secondary-receiver ]

no remotefile format

no
Resets the remote file naming convention to the system default.

format format_string
Default: “%date%-%time%”
Specifies the naming convention format to use. format_string must be from 1 to 127 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described in the Schema Format String Syntax section.

Important: The remote file naming format should only use static text and bulk statistic variables to avoid any possible file creation issues on the receivers.

The following variables are supported:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>The UTC date that the collection file was created in YYYYMMDD format where YYYY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>date3</td>
<td>The UTC date that the collection file was created in YYMMDD format where YY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>host</td>
<td>The system hostname that created the file</td>
<td>String</td>
</tr>
<tr>
<td>sysuptime</td>
<td>The uptime (in seconds) of the system that created the file.</td>
<td>32-bit signed</td>
</tr>
<tr>
<td>time</td>
<td>The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.</td>
<td>String</td>
</tr>
</tbody>
</table>
both-receivers | primary-receiver | secondary-receiver

Set the remote file creation target to both receivers, primary receiver or secondary receiver. Default: Both receivers.

**Usage**

Set the remote file naming format to ensure consistent data file naming across a network or adjusting a single system’s format for easy identification.

This command specify whether the format should be used in conjunction with both receivers, only the primary receiver, or only the secondary receiver.

**Important:** For redundant receivers, the filenames for the output data files are applied when the information is first gathered. If the name format is modified, the change takes effect for the next data set. The current data set name remains unchanged, even if has not yet been transferred.

**Example**

```plaintext
remotefile format simpleFormat
remotefile format "%host%-%date%-%time%" [both-receivers]
remotefile format "%host%-%date%" [primary-receiver]
no remotefile format
```
rp schema

This command configures R-P bulk statistics schema.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

rp schema

no rp schema

Syntax:

rp schema

no

Remove the specified schema.

schema_name

Specify the schema name.

schema_name must be an alpha and/or numeric string of 1 through 31 characters in length.

format

Specify the schema format.

format_string must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for R-P bulk statistics collection. Multiple PDSN service schemas can be created to categorize PDSN service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PDSN service schemas, re-issue the rp schema command using a different schema name.

Example

To create an PDSN-level schema called pdsn servicestats that specifies a schema format of:

Date: date
Time: time
Number of Authentication Denials: deny-auth

Use the following command:

rp schema rpservicestats format "Date: %date%
Time: %time%
Number of Authentication Denials: %deny-auth%"
**sample-interval**

This command configures the time interval between collecting local statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sample-interval minutes

minutes
```

Specifies the frequency of polling for local statistics.

*minutes* must be an integer from 1 through 1440.

**Usage**

Adjust the sampling interval to tune the system response as shorter periods can cause undue system overhead whereas longer periods have less of a statistical importance when analyzing data.

The system is shipped from the factory with the sampling interval set to 15 minutes.

**Example**

```
sample-interval 120
```


**sccp schema**

This command configures the statistics collection schema for the Signalling Connection Control Part function (SCCP).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
sccp schema schema_name format format_string
no sccp schema schema_name
```

**no**

Removes the specified SCCP schema from statistics collection.

```plaintext
schema_name
```

Specifies the name to use to refer to the schema and associated format string. `schema_name` must be from 1 to 31 alpha and/or numeric characters.

```plaintext
format format_string
```

Specifies the naming convention format to use. `format_string` must be from 1 to 3599 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described by `Schema Format String Syntax`.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*. 
schema

This command configures the system-level bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
schema schema_name format format_string
no schema schema_name
```

**no**

Removes the specified schema.

```
schema_name
```

Specifies the schema name.
`schema_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

```
format format_string
```

Specifies the schema format.
`format_string` must be an alpha and/or numeric string of 1 through 3599 characters in length, and cannot include spaces or must be a quoted string. For syntax details, see [Schema Format String Syntax](#) section.

### Important:
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for system-level bulk statistics collection. Multiple schemas can be created to categorize system-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple system schemas, re-issue the `schema` command using a different schema name.

**Example**
The following command creates a schema called `systemstats1` that records the number of current Simple IP and the number of current Mobile IP sessions:

```
schema systemstats1 format "@sess-cursipconn@ - @sess-curmipconn@"
```

To create a system-level schema called `bulksysstats` that specifies a schema format of:

*Number of currently active sessions: sess-curactcall*
*Number of currently dormant sessions: sess-curdormcall*

Use the following command:
schema bulksysstats format "Number of currently active sessions: %sess-curactcall\nNumber of currently dormant sessions: %sess-curdormcall\n"
sgsn schema

This command configures the statistics collection schema for the SGSN services.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
sgsn schema schema_name format format_string

no sgsn schema schema_name
```

- **no**
  Removes the specified SGSN schema from statistics collection.

- **schema_name**
  Specifies the name to use to refer to the schema and associated format string. `schema_name` must be from 1 to 31 alpha and/or numeric characters.

- **format format_string**
  Specifies the naming convention format to use. `format_string` must be from 1 to 3599 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described by Schema Format String Syntax.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
sgtp schema

This command configures the statistics collection schema for the SGSN’s GTP-C and GTP-U activity.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sgtp schema schema_name format format_string
no sgt p schema schema_name
```

- **no**
  - Removes the specified SGTP schema from statistics collection.

- **schema_name**
  - Specifies the name to use to refer to the schema and associated format string. `schema_name` must be from 1 to 31 alpha and/or numeric characters.

- **format format_string**
  - Specifies the naming convention format to use. `format_string` must be from 1 to 3599 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described by [Schema Format String Syntax](#).

**Important:** For a complete list of the statistics that are supported for this schema, refer to the [Statistics and Counters Reference](#).
ss7link schema

This command configures the collection schema for the SS7 Link services statistics.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
ss7link schema schema_name format_string
no ss7link schema schema_name
```

- **no**
  Removes the specified SS7 Link schema from statistics collection.

- **schema_name**
  Specifies the name to use to refer to the schema and associated format string. `schema_name` must be from 1 to 31 alpha and/or numeric characters.

- **format format_string**
  Specifies the naming convention format to use. `format_string` must be from 1 to 3599 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described by Schema Format String Syntax.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
ss7rd schema

This command configures the collection schema for the SS7 Routing Domain services statistics which include the statistics for Stream Control Transmission Protocol (SCTP) activities, the statistics for MTP3, and M3UA data activity.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ss7rd schema schema_name format format_string
no ss7rd schema schema_name
```

- `no`
  Removes the specified SS7 routing domain schema from statistics collection.

- `schema_name`
  Specifies the name to use to refer to the schema and associated format string. `schema_name` must be from 1 to 31 alpha and/or numeric characters.

- `format format_string`
  Specifies the naming convention format to use. `format_string` must be from 1 to 3599 alpha and/or numeric characters with no spaces or as a quoted string. The format string syntax is described by [Schema Format String Syntax](#).

**Important:** For a complete list of the statistics that are supported for this schema, refer to the [Statistics and Counters Reference](#).
show variables

Displays the bulk statistics variable information.

Product
All

Privilege
Security Administrator, Administrator

Syntax

show variables [ [ apn | asngw | bcmcs | card | closedrp | common | context | cscf | ecs | fa | gprs | gtpc | gtpp | ha | ippool | ipsg | lac | pdif | port | ppp | radius | rp | sccp | sgsn | sgtp | ss7rd | ss7link | system | vpn | obsolete ] ]

Displays only the variables for the specified schema.
If the obsolete keyword is used, obsolete (but still available) schema variables are displayed. An asterisk (*) is displayed next to schema variables that have been obsoleted.
For information on available schemas, refer to the Bulk Statistics Configuration Mode Commands chapter.

Usage

Use this command to list supported bulk statistic variables. Variables can be listed for a specified schema. If no schema is specified, all supported variables are listed on a per-schema basis.

Example

The following command displays the bulkstat variables only for the card schema:

show variables card
transfer-interval

Configures the frequency of transfer of collected statistics to the receiver.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
transfer-interval minutes
```

*minutes*

Specifies the number of minutes between the transfer of collected statistics to the receivers. *minutes* must be an integer from 1 through 999999.

**Usage**

Modify the transfer interval based upon the number of sessions per second. As the number of session requests a second increases it may become necessary to increase the transfer interval to reduce the processing overhead frequency for statistics delivery. This is tempered by the impact reduced resolution of statical data has on usefulness of data when the interval gets larger than the least busy hours and most busy hours of the day.

The system is shipped from the factory with the transfer interval set to 480 minutes.

**Example**

```
transfer-interval 1440
```
Chapter 31
Card Configuration Mode Commands

The Card Configuration Mode is used to create and manage the different types of physical cards in the chassis.
**aps**

This command configures automatic protection switching (APS) features for SONET/SDH line cards - OLC2 or CLC2.

**Important:** This feature is not yet fully supported.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**1+1**

Linear 1+1 Uni-directional APS type redundancy:
- Linear means th

**1:1**

APS type Linear 1:1 Bi-directional.

**non-revertive**

**revertive**

**-noconfirm**

Instructs the system to execute the command without additional prompting for command confirmation.

**aps 1+1**
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
end
```

Usage
Change the command mode back to the Exec mode.

Example

```
end
```
exit

Exits the current mode, card configuration mode, and returns the CLI session to the previous mode, global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the Global configuration mode.

**Example**

```
exit
```
framing

This command configures the type of framing used for the signaling generated on a specific type of line card.

Product
All

Privilege
Security Administrator, Administrator

Syntax

framing { ethernet | sdh [ ds1 | e1 ] | sonet [ ds1 | e1 ] | unspecified } [ -noconfirm ]
default framing [ -noconfirm ]

default
Resets the framing generated by the card to the default for the particular card type.

ethernet
Configures the system to use Ethernet framing for this line card. This type of framing can only be used on an ethernet card.
Default: Ethernet framing type is the default for an Ethernet line card.

**Important:** Using this keyword with an OLC/OLC2 or CLC/CLC2 would take the card offline.

sdh [ ds1 | e1 ]
Configures the system to use SDH signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.

**Important:** Using this keyword with an Ethernet line card would take the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.

ds1 - configures the card to support a DS1/T1.
e1 - configures the card to support an E1. This is the default for SDH.

sonet [ ds1 | e1 ]
Configures the system to use SONET signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.
Default: SONET is the default framing type for an OLC/OLC2 or CLC/CLC2 line card.

**Important:** Using this keyword with an Ethernet line card would take the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.
ds1 - configures the card to support a DS1/T. This is the default for SONET.
e1 - configures the card to support an E1.

**unspecified**
Configures the system to use the default framing type for the particular line card resident in the identified slot.

**-noconfirm**
Instructs the system to execute the command without additional prompting for command confirmation.

**Usage**
Use the `framing` command to identify the type of signal framing to be used by the line card in the identified slot.
It should be noted that each type of line card uses a different type of signal framing. If the wrong type of framing is configured for a line card, the line card will be taken offline.

**Important:** This command is not supported on all platforms.

**Example**
The following command could be used to configure SDH signal framing on a CLC2. By not including the path-type, the default of E1 will automatically be included in the card’s framing configuration:

```
framing sdh
```
header-type

This command defines the size of the header frame for Frame Relay transmissions over a CLC or CLC2 channelized line card.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

header-type header-size [ -noconfirm ]
default header-type [ -noconfirm ]

- default
  Resets the configuration to the default header size of 2-bytes.

- header-size
  This sets the size, number of bytes, for the header frame. header-size must be either 2-bytes or 4-bytes.

- -noconfirm
  Instructs the system to execute the command without additional prompting for command confirmation.

Usage
Use this command to set the size of the header frame for Frame Relay messages emanating from the line card. The size (2-bytes or 4-bytes) determines the amount of information that can be transmitted in that first information frame.

Important: Not supported on all platforms

Example
Set the header to the smallest size.

  header-type 2-byte
**initial-e1-framing**

Configures the type of framing mode that will be initially available at the time the line card boots.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
initial-e1-framing [ crc4 | standard ]
default initial-e1-framing
```

- **default**
  Returns the configuration to CRC4 as the default type.

- **crc4**
  Accepts the default CRC4, in the configuration, as the initial at-boot framing mode.

- **standard**
  Accepts the **standard** mode as the initialization framing mode.

**Usage**

For a CLC-type line card, the default E1 framing mode is "CRC4". When a card reboots, all E1s are initialized with "CRC4" framing mode and then switch to the configured framing mode. With this keyword, the user has the option to choose the initialization framing mode.

**Important:** Only supported on CLC/CLC2

**Example**

```
initial-e1-framing standard
```
link-aggregation

Configures the link-aggregation system-priority for a Quad Gig-E line card (QGLC). This parameter is usually changed to match the feature requirements of the remote switch.

Product
WiMAX, PDSN, HA, FA, GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
link-aggregation { system-priority priority | toggle-link } [ -noconfirm ]
{ default | no } link-aggregation { system-priority | toggle-link } [ -noconfirm ]

default
Resets the configuration to the default.

link-aggregation system-priority priority
This command sets the system priority used by LACP to form the system ID. priority is a hex value in the range of 0x0000 to 0xFFFF.
Default system priority value is 0x8000 (32768).

toggle-link
When enabled, port line down and port link up events are generated.
Default is disabled.

-noconfirm
Instructs the system to execute the command without additional prompting for command confirmation.

Usage
This value is combined with the Master port’s MAC address to form the system ID. A system is a PSC or PSC2 and its associated QGLC(s) The highest system ID priority (the lowest number) handles dynamic changes.
For additional usage and configuration information for the link aggregation feature, go to Configuring Link Aggregation in the System Administration Guide.

Important: Not supported on all platforms

Example
The following command configures the link aggregation system-priority to 10640:

```
link-aggregation system-priority 0x2990
```
link-aggregation
mode

Sets the application Processor Card’s current administrative state to active or standby.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mode { active [ pac | psc] | standby } [ -noconfirm ]
default mode [ -noconfirm ]
```

**Important:** This command results in a migration of processes if the default mode for a card is different than the current state of the card.

**active [ pac | psc]**
Defines which card type is to be switched from standby to active state. If a card is present in the slot, the Processing Card is automatically selected depending upon the type of card. If no card is present in the slot, Processing Card is assumed.

*pac*: Identifies a PAC

*psc*: Identifies a PSC or PSC2

**standby**
Sets the PSC, or PSC2 in the slot to standby mode.

**Caution:** Switching an active PSC/PSC2 to standby deletes all port configurations, including bindings, for the attached line cards.

**-noconfirm**
Instructs the system to execute the command without additional prompting for command confirmation.

**Usage**
Set the desired mode of mated cards. The card targeted for maintenance is placed in the standby state first. The setting of the mode determines which PSCs or PSC2s are to be active and which are to be the standby cards for redundancy. Use this command to configure the set of active and standby PSCs/PSC2s. The
application processor card’s standby priority is then used in conjunction with the set of standby PSCs or PSC2s to determine the order in which the standby cards are used for redundancy support.

**Important:** Not supported on all platforms

**Important:** This command results in a migration of processes if the mode specified for the card is different than the current state of the card.

**Example**
The following commands set the state of a card to active and standby, respectively.

```
mode active
mode standby
```
redundancy

Configures the type of redundancy for a line card or SPIO.

**Product**
PDSN, FA, HA, GGSN, SSGN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redundancy { card-mode | mixed-mode | port-mode | pseudo-aps-mode } [-noconfirm ]
```

```
default redundancy [ -noconfirm ]
```

```
default
Restores redundancy to port-mode type redundancy.
```

```
card-mode
Specifies no port redundancy is used. This is used mostly for legacy products.
```

```
mixed-mode

port-mode
Enables port redundancy on line cards or on SPIO cards.
This is the default setting used by the system.
```

**Important:** Port-type redundancy does not affect line card failover/redundancy operations.

```
pseudo-aps-mode
```

**Important:** This feature is not yet fully supported.

With release 8.1 and higher, this keyword enables pseudo-APS type port redundancy on OLC2/CLC2 line cards.

```
-noconfirm
Instructs the system to execute the command without additional prompting for command confirmation.
```

**Usage**
Use this command to configure redundancy on a line card (LC) or a SPIO card. With port-mode enabled, if an external network device or cable failure occurs that causes a link down failure on the port, the redundant port is used.
**Important:** Not supported on all platforms

**Important:** You do not need to enter this command for each LC or SPIO card, as the system intuitively understands that if the command is entered for an active LC or SPIO card, the standby LC or SPIO card switches to operate in the same mode. For example, entering the `port-mode` command for an LC in slot 17 automatically enables a redundant LC in slot 33 for port redundant operation.

**Example**
The following command sets the redundancy mode to port redundancy.

```
redundancy port-mode
```
service-type

This command configures the type of service the CLC or CLC2 line card will support.

**Important:** Supported in software releases 8.1 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
service-type { frame-relay | mtp2 | pwe3-cesopsn | unspecified } [ -noconfirm ]
default service-type [ -noconfirm ]
```

- **default**
  - Returns the card configuration to ‘unspecified’.

- **frame-relay**
  - Configures the card to operate in Frame Relay service mode.

- **mtp2**
  
  **Important:** MTP2 functionality is not yet supported.

  Enables MTP2 type service to support narrowband transmissions.

- **pwe3-cesopsn**

  **Important:** pwe3-cesopsn functionality has been replaced by mtp2.

- **unspecified**
  - This is the default mode for a CLC or CLC2 linecard.

**Important:** You must configure the linecard to one of the available service types or the card will not function.

- **-noconfirm**
  - Instructs the system to execute the command without additional prompting for command confirmation.

**Usage**
Use this command to configure the operational service mode for the channelized line card - CLC or CLC2. Once you select the service-type, refer to the Channelized Port configuration mode chapter to review the commands needed to configure the parameters for the port.

Example

```
    service-type frame-relay
```
shutdown

Configures a card for active service or terminates all processes on the card.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] shutdown
```

- `no shutdown` enables the card.

Enter only the `shutdown` keyword to shut the card down.

**Usage**
Shut down a card to remove it from service or to enable a card to put it into service.

**Important:** Do not use this command to remove a card from service for maintenance. Use the command `card halt` to remove a card for service to avoid changing or deleting the active-mode configuration. See the Exec Mode chapter.

**Important:** Not supported on all platforms

**Example**
The following commands shutdown the card and switch a card to online, respectively.

```
shutdown
no shutdown
```
Chapter 32
Channelized Port Configuration Mode Commands

The channelized port configuration mode provides the commands to create, configure, bind, and manage the Frame Relay service ports on the channelized line card.

**Important:** Before using these commands, card framing should be configured for either SDH or SONET with the framing command described in the Card Configuration Mode chapter.

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

Entering this command disables the alarm detection for designated sets of alarms.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
alarm-disable { all | ds1-e1 | none | sonet-sdh }
[ no | default ] alarm-disable
```

- **no**
  Deletes the disable configuration.

- **default**
  Returns the settings for disabling alarms to the system default.

- **all**
  Disables detection of all SONET/SDH and DS1/E1 alarms.

- **ds1-e1**
  Disables detection of the DS1/E1 alarms.

- **none**
  None of the alarm detection is disabled so that all DS1/E1 and SONET/SDH alarms are detected.

- **sonet-sdh**
  Disables detection of SONE/SDH alarms.

Usage
Configure selected alarm detection for the port.

Example
Enter the following command to enable DS1/E1 and SONET/SDH alarm detection.

```
alarm-disable none
```
alarm-soak-timer

This command sets the timer for the duration that a detected alarm will be soaked before the alarm is reported.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

alarm-soak-timer  seconds

default alarm-soak-timer

Usage

Configures the delay before reporting detected alarms.

Example

Configure a 20 second alarm report delay.

    alarm-soak-timer 20
**clock-source**

This command sets the source of the port’s transmit clock.

<table>
<thead>
<tr>
<th><strong>Important:</strong></th>
<th>This command is only available for releases 8.1 or higher.</th>
</tr>
</thead>
</table>

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
clock-source { internal-timing | loop-timing }
```

default clock-source

- **default**
  Using this command combination sets the port clock source to internal timing.

- **internal-timing**
  Sets the port clock to derive timing from the recovered receive clock.

- **loop-timing**
  Sets the port clock to transmit in sync with the system timing.

**Usage**
Use this command for either SONET or SDH channelized (Frame Relay) ports on the SGSN.

**Example**
The following command resets the transmit clock source to internal timing.

```
default clock-source
```
description

Defines descriptive text that provides useful information about the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

description text

no description

no
Erases the port’s description from the configuration file.

text

text must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage
Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters.

Example

description samplePortDescriptiveText

description "This is a sample description"
dlci

Identifies a data link connection identifier (DLCI), a frame relay logical connection, and binds it with a specific channelized path configuration. Once the DLCI is bound to the path, the system enters DLCI configuration mode.

**Important:** The `path` command must be configured prior to attempting configuration with the `dlci` command.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
dlci path path_id { ds1 | e1 } connects { dlci dlci_id | timeslots slot# dlci dlci_id }  
no dlci path path_id { ds1 | e1 } connects  
```  

**no**

Disables the configured DLCI.

**path path_id**

Identifies a specific path configuration, set with the `path` command in this configuration mode, that will be associated with a DLCI.

- `path_id`: must be an integer from 1 to 3.

**ds1 connects | e1 connects**

Selects the framing speed for the connection.

- **DS1**: is associated with North American networks and would be the best choice to work with the SONET framing selected with the `card` configuration command.
- **connects**: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.

- **E1**: is associated with European networks and would be associated with the SDH framing selected with the `card` configuration command.
- **connects**: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

**dlci dlci_id**

Identifies a specific Frame Relay PVC DLCI to associate with the path.

- `dlci_id`: an integer from 16 to 991.

**timeslot slot#**

Identifies one of the timeslots within a timeslot group configured with the `path` command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.
**Usage**

Associating a routing path with a specific frame relay DLCI is a significant part of the process for defining the frame relay interface.

**Example**

Associate path 1 with DLCI 123.

```
dlci path 1 ds1 21 dlci 123
```
**end**

Exits the Channelized Port configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the Channelized Port configuration mode and returns to the Global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the Global configuration mode.
frame-relay

Configures the parameters for the Frame Relay connections for E1, DS1 and fractional E1 ports created with the `path` command. Frame

**Important:** The `path` command must be configured prior to attempting configuration with the `frame-relay` command.

**Product:**
SGSN

**Privilege:**
Security Administrator, Administrator

**Syntax**

```
frame-relay path path_id { ds1 connects | el connects } timeslot slot# [
  intf-type intf_type ] [ lmi_type lmi_type ]
```

`path  path_id`

Identifies a specific path configuration, set with the `path` command in this configuration model. `path_id` must be an integer from 1 to 3.

`ds1 connects | el connects`

Selects the pipe splitting for the connection. **DS1**: Is associated with North American networks and would be the best choice to work with the SONET framing selected with the `card` configuration command. DS1 splits the path into 28 logical connections. connects Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.

**E1**: is associated with European networks and would be associated with the SDH framing selected with the `card` configuration command. E1 splits the path into 21 logical connections.

connects Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

`timeslot  slot#`

Identifies one of the timeslots within a timeslot group configured with the `path` command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.

`slot#`: Must be an integer from 1 to 31.

`intf-type  intf_type`

Selecting the interface type specifies signaling parameters for the DLCI, options include:

- `dce`: Selects data circuit-terminating equipment -type signaling.
- `dte`: Selects data terminal equipment -type signaling.
- `nmi`: Selects the network-to-network interface

Default: DTE for Release 8.0
Default: DCE for Release 8.1
frame-relay lmi_type lmi_type

Default: none.

Line management options include:

- `ansi` - ANSI ANNEXED LMI, may include option:
- `cisco` - Cisco/Gang Of Four LMI
- `none` - LMI Disabled
- `q933a` - Q.933A LMI

Any of the above LMI types can take one or more additional options

- `n391 value` - Number of keep exchanges before requesting a full status message. Default is 6. `value` must be an integer from 1 to 255.
- `n392 value` - Error Threshold value. Default is 2. `value` must be an integer from 1 to 10.
- `n393 value` - Monitored events count value. Default is 2. `value` must be an integer from 1 to 10.
- `t391 value` - Timer to send messages. Default is 10. `value` must be an integer from 5 to 30.
- `t392 value` - Polling verification timer value. Default is 15. `value` must be an integer from 5 to 30.

Usage

Use this command to define LMI type and timers and to associate time group 2 with the Frame Relay connection.

Example

frame-relay path 1 e1 3 timeslot 2
**hopath-sdsf**

Configures the high-order path for SDSF bit error rate (BER) thresholds.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
hopath-sdsf hopath_value
```

*hopath_value*

- 0: Disabled
- 1 - 1.E-03
- 2 - 1.E-04
- 3 - 1.E-05
- 4 - 1.E-06
- 5 - 1.E-07
- 6 - 1.E-08
- 7 - 1.E-09
- 8 - 1.E-10

**Usage**

Sets a standard option for the high-order path for SDSF.

**Example**

```
hopath-sdsf 1
```
line-timing

This command enables the SPIO to recover transmit timing source via line attached to the selected port. By default, line-timing is not enabled.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
[ no ] line-timing

no
Disables line-timing as the source for the transmit clock.

Usage
The port must be enabled (with the no shutdown command) to enable recovery of timing source via the line. As well, the card’s slot number must be entered in the recover line# command of the BITS port configuration mode.

Example
Disable timing clock recovery on this port.

no line-timing
**loopback**

Configures the type of loopback mode used for diagnostic testing.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
loopback { ds1-e1-diag | ds1-e1-line | none | sonet-sdh-diag | sonet-sdh-line }
```

- **ds1-e1-diag**
  Enables a system generated diagnostic lookback signal at the DS1/E1 layer.

- **ds1-e1-line**
  Loops back a network diagnostic signal at the DS1/E1 layer.

- **none**
  Stops diagnostic loopback signalling.

- **sonet-sdh-diag**
  Enables a system generated diagnostic lookback signal at the SONET/SDH layer.

- **sonet-sdh-line**
  Loops back a network diagnostic signal at the SONET/SDH layer.

**Usage**

Setup diagnostic loopback signals for troubleshooting purposes.

**Example**

```
loopback ds1-e1-diag
```
lopath-sdsf

Configures the low-order path for SDSF bit error rate (BER) thresholds.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
lopath-sdsf  lopath_value
```

<table>
<thead>
<tr>
<th>lopath_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: Disabled</td>
</tr>
<tr>
<td>1.E-03</td>
</tr>
<tr>
<td>1.E-12</td>
</tr>
<tr>
<td>1.E-04</td>
</tr>
<tr>
<td>1.E-05</td>
</tr>
<tr>
<td>1.E-06</td>
</tr>
<tr>
<td>1.E-07</td>
</tr>
<tr>
<td>1.E-08</td>
</tr>
<tr>
<td>1.E-09</td>
</tr>
<tr>
<td>1.E-10</td>
</tr>
<tr>
<td>1.E-11</td>
</tr>
</tbody>
</table>

Usage

Sets a standard option for the low-order path for SDSF.

Example

```
lopath-sdsf  1
```
mtp2

Creates an MTP2 configuration instance for the port.

**Important:** The port DS1/E1 tributaries must be configured using the `path` command prior to creating a port MTP2 configuration.

**Important:** The MTP2 feature is not yet fully supported and so the command is not yet fully functional. Please ignore this keyword, at this time, while configuring the channelized port.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator
path

This command configures the parameters that define the routing path for a DLCI. It must match with the DLCI configuration parameters. The values entered with these commands should be noted as they will be needed to configure the `frame-relay` and `dltci` commands also in this configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
path path_id { ds1 connects | e1 connects } frame-mapping multiplexing
index# index# framing mode mapping-mode { bit-sync | byte-sync } [ timeslots
slot# [ slot# ] | frame-relay [ intf-type intf_type [ lmi_type lmi_type ] ] ]
```

```
no path path_id { ds1 | e1 } connects
```

**no**
Deletes the routing path entry from the configuration.

```
path path_id
```

Identifies a specific path configuration that will be associated with a DLCI. The `path_id` must be an integer from 1 to 3.

```
ds1 connects | e1 connects
```

Selects the channelization for the connection.

**DS1** (AKA: T1) is associated with North American networks and would be the best choice to work with the SONET (can also work with SDH) framing selected with the `card` configuration command. DS1 splits the path into 28 logical connections.

**connects:** Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.

**E1** is associated with European networks and would be associated with the SDH (can also work with SONET) framing selected with the `card` configuration command. E1 splits the path into 21 logical connections.

**connects:** Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

```
frame-mapping
```

Frame mapping sets the channelization according to the national standards that correlate with the framing/speed standards. This option selects the mapping of containers (C), virtual containers (VC), tributary units (TU), and tributary unit groups (TUG), that is appropriate for the channel characteristics:

**`tu11-au3`**: Appropriate for DS1 in SDH. Maps as follows: AU-3—VC-3—m#—TUG-2—m#—TU-12—VC-12—C-12

**`tu11-au4`**: Appropriate for DS1 in SDH. Maps as follows: AU-4—VC-4—TUG-3—m#—TUG-2—m#—TU-11—VC-11—C-11
Channelized Port Configuration Mode Commands

- **tu12-uu3**: Appropriate for E1 in SDH. Maps as follows AU-3—VC-3—m#—TUG-2—m#—TU-12—VC-12—C-12
- **tu12-uu4**: Appropriate for E1 in SDH. Maps as follows AU-4—VC-4—TUG-3—m#—TUG-2—m#—TU-12—VC-12—C-12

Frame Mapping for E1 and DS1 to STM-n Interfaces

- **vt1.5**: Only appropriate for DS1 in SONET framing.
- **vt2**: Only appropriate for E1 in SONET framing.

```
multiplexing index# index#
index#: TUG-2 index - Must be an integer from 1 to 7 to identify a multiplex channel between TUG-2 and VC-3 (E1) or TUG-3 (DS1).
index#: TU index - Must be an integer from 1 to 4 (DS1) or 1 to 3 (E1) to identify a multiplex channel between TU-11 (DS1) and TUG-2 or between TU-12 (E1) and TUG-2.
```

```
framing mode
Defines the framing modes to be used for the channelization to E1 or T1 of the (optical) port.
- options for E1:
  - **cas**: standard mapping with CAS
  - **cas-crc4**: CRC4 mapping with CAS
  - **crc4**: CRC4 mapping
  - **standard**: mapping
- options for DS1:
  - **esf**: extended superframe mapping
  - **sf**: superframe mapping
  - option for either E1 or DS1:
    - **unframed
```

```
mapping-mode
- **bit-sync
- **byte-sync
```
timeslots timeslots
Defines up to 8 timeslot groupings for multiple fractional DS1/E1 channels. Each slot is 2.048/32 Mbytes. Slots 0 and 16 are reserved for synchronization and alarms. Slots 1-15 and 17-31 are used for data. Timeslots must be unique -- a timeslot can not be used in more than one grouping.

timeslots: Must be an integer from 1 to 31. Timeslot groups are separated by spaces and can consist of a single slot and/or a range indicated with a hyphen. Example: 3,7-10 is a single fractional group. NOTE there is no space after the comma. Timeslots must be unique -- a timeslot can not be used in more than one grouping.

frame-relay
Enables definition of a Frame Relay connection with the frame-relay command.

Important: For release 8.1 and higher, this feature has been moved to the frame-relay command.

intf-type intf_type
Selecting the interface type specifies signaling parameters for the DLCI, options include:
  •dce: Selects data circuit-terminating equipment -type signaling.
  •dte: Selects data terminal equipment -type signaling.
  •nni: Selects the network-to-network interface
Default: DTE for Release 8.0
Default: DCE for Release 8.1

Important: For release 8.1 and higher, this feature has been moved to the frame-relay command.

lmi_type lmi_type
Default: none.
Line management type options include:
  •ansi - ANSI ANNEXED LMI, may include option:
  •cisco - Cisco/Gang Of Four LMI
  •none - LMI Disabled
  •q933a - Q.933A LMI
Any of the above LMI types can take one or more additional options
  •n391 value - Number of keep exchanges before requesting a full status message. Default is 6. value must be an integer from 1 to 255.
  •n392 value - Error Threshold value. Default is 2. value must be an integer from 1 to 10.
  •n393 value - Monitored events count value. Default is 2. value must be an integer from 1 to 10.
  •t391 value - Timer to send messages. Default is 10. value must be an integer from 5 to 30.
  •t392 value - Polling verification timer value. Default is 15. value must be an integer from 5 to 30.

Important: For release 8.1 and higher, this feature has been moved to the frame-relay command.
Usage
Defines the signaling characteristics of a frame relay connection or timeslots for a fractional connection. Use this command to create E1 ports or fractional E1 ports. Fractional E1 ports are created with the timeslot definitions. The fractional E1 port can consist of one or more or all of the timeslots.

Example
In the first example, define timers for the q933a LMI-type.

```
path 1 e1 1 tu12-au4 1 1 framing crc4 mapping-mode bit-async
framing 10 10
```

The next example defines 3 groups of fractional timeslots with group 1 having slots 1-5 and 8, group 2 having slot 22-25, and group 3 having slots 31.

```
path 1 e1 1 tu12-au3 1 1 framing cas mapping-mode bit-async
timeslots 1-5,8 22-25 31
```
preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the LC in slot 17 while ports 5 through 8 are “preferred” on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

preferred slot slot#

no preferred slot

<table>
<thead>
<tr>
<th>slot#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the physical slot in the chassis where the line card is installed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables revertive, or auto-recovery, operation for the port.</td>
</tr>
</tbody>
</table>

Usage
This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically. Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

Example

preferred slot 17
pwe3-cesopsn

This command has been replaced by the mt2 command.

Product
SGSN

Privilege
Security Administrator, Administrator
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the **no** keyword enables the port.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
shutdown
no shutdown
```

**Usage**
Shut down a port prior to re-cabling and/or other maintenance activities.
This command with the **no** keyword is required to bring a port into service.

**Example**

```
shutdown
no shutdown
```
**snmp trap link-status**

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
snmp trap link-status

no snmp trap link-status
```

- **no**

  Disables the sending of traps for link-status changes.

**Usage**

Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

**Example**

```plaintext
snmp trap link-status

no snmp trap link-status
```
**threshold high-activity**

Configures the port’s high and low activity thresholds.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold high-activity high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 50
Sets the threshold for the highest percentage of port activity that must be met or exceeded, within the polling interval, to generate an alert or alarm.

`high_thresh`% can be configured to any integer value between 0 and 100.

**clear low_thresh**
Default: 50
Sets the threshold for the lowest percentage level of port activity that must be met to generate and send a clear alarm. If port activity does not drop to or below this threshold then the alarm is maintained.

`low_thresh`% can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port ≥ High Threshold
- **Clear condition:** Actual percent utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**
The following command configures a high port utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
channelized port configuration mode commands

threshold high-activity
threshold monitoring

Enables thresholding for port-level values.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

threshold monitoring

no threshold monitoring

no
Disables threshold monitoring for port-level values. This is the default setting.

Usage
Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference. The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until a the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
This command enables thresholding for port-level values. Refer to the `threshold high-activity threshold rx-utilization` and `threshold tx-utilization` commands in this chapter for information on configuring these values. In addition refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference for information on configuring the polling interval over which these values are monitored.
threshold rx-utilization

Configures thresholds for receive-port utilization.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
threshold rx-utilization high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 80
The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

**clear low_thresh**
Default: 80
Allows the configuration of the low threshold.
The low threshold receive port utilization percentage that maintains a previously generated alarm condition.
If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:
- **Enter condition:** Actual percent utilization of a port for received data ≥ High Threshold
- **Clear condition:** Actual percent utilization of a port for received data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold_poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold_monitoring` command in this chapter to enable thresholding for this value.

**Example**
The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```
threshold tx-utilization

Configures thresholds for transmit port utilization.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
threshold tx-utilization high_threshold [ clear low_threshold ]

<table>
<thead>
<tr>
<th>high_threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 80</td>
</tr>
</tbody>
</table>
| The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage can be configured to any integer value between 0 and 100.

<table>
<thead>
<tr>
<th>clear low_threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 80</td>
</tr>
</tbody>
</table>
| Allows the configuration of the low threshold. The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:
- **Enter condition:** Actual percent utilization of a port for transmit data ≥ High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

Example
The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```
**toh-sdsf**

Configures the line SDSF bit error rate (BER) thresholds.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
toh-sdsf toh_value
```

**toh_value**

- 0: Disabled
- 1 - 1.E-04
- 2 - 1.E-05
- 3 - 1.E-06
- 4 - 1.E-07
- 5 - 1.E-08
- 6 - 1.E-09
- 7 - 1.E-10
- 8 - 1.E-11

**Usage**

Sets a standard option for the line SDSF BER.

**Example**

```
toh-sdsf 1
```
vc-mapping

This command has been deprecated. Go to the frame-mapping keyword in the path command to configure this functionality.
Chapter 33
Charging Action Configuration Mode Commands

The Charging Action Configuration Mode is used to create and manage Charging Action services.

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

This command configures billing actions for packets that match ruledefs.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
billing-action { edr edr_format_name [ wait-until-flow-ends ] | egcdr | exclude-from-udrs | radius | rf } +
```

```
no billing-action [ edr | egcdr | exclude-from-udrs | radius | rf ] +
```

no

Disables billing-action configuration for the charging action.

Specifying one of the optional keywords disables that functionality. If you want to disable all billing-action functionality, do not specify any of the optional keywords.

```
edr edr_format_name [ wait-until-flow-ends ]
```

Enables EDR billing for packets matching this charging action.

`edr_format_name` must be the name of an existing EDR format, and must be a string of 1 through 63 characters in length.

**Important:** If the EDR format name supplied here is not configured in the EDR Format Configuration Mode, or has been deleted, the system accepts it without applying any EDR format for the billing action in this ACS service.

If this option is configured, the system generates an EDR immediately when a packet is received and it matches a ruledef that is associated with this charging action. Other events configured for flow end-condition, flow action, termination, and/or session control also creates the triggers for EDR generation.

`wait-until-flow-ends`: By default, the EDR is generated immediately after a ruledef hit results in this charging action. When this keyword is specified, no EDR is generated on a ruledef hit. When the flow ends, an attempt is made to generate an EDR with the format specified.

```
egcdr
```

Enables eG-CDRs billing for packets matching this charging action.

If this option is configured, system generates an eG-CDR when the subscriber session ends or an interim trigger condition occurs. The interim triggers are configurable in the Rulebase Configuration Mode. In addition, whenever there is an SGSN-to-SGSN handoff the system treats that as a trigger.

To generate an eG-CDR the `accounting-mode` CLI command in the APN Configuration Mode must be configured with the “none” option.

The format of enhanced G-CDRs is controlled by the `inspector` CLI command in Context Configuration Mode.

```
exclude-from-udrs
```

Default: Disabled.
By default, statistics are accumulated on a per content ID basis for possible inclusion in UDRs. The `exclude-from-udrs` keyword causes the system to not include the packet’s statistics in UDRs. When this option is disabled, (the default setting) UDRs will be generated based on the udr format declared in the rulebase.

**radius**

Default: Disabled.
Enables billing action as RADIUS CDRs for packets matching this charging action, and the data packet statistics will be included in the postpaid RADIUS accounting.

**rf**

Enables Rf accounting. Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the `billing-records` CLI in the Rulebase Configuration Mode.

**Usage**

Use this command to enable an EDR, eG-CDR and/or RADIUS CDR type of billing for content matching this charging action.

**Example**
The following command enables the EDR billing type with EDR format `charge1_format`:

```
billing-action edr charge1_format
```
cca charging

This command enables Credit Control Application and configures RADIUS/Diameter prepaid charging behavior.

Product
All

Privilege
Security Administrator, Administrator

Syntax

cca charging credit [ preemptively-request | rating-group coupon_id ]
{ default | no } dcca charging

no
Disables RADIUS/Diameter Prepaid Credit Control Charging.

default
Disables RADIUS/Diameter Prepaid Credit Control Charging.

credit
Specifies RADIUS/Diameter Prepaid Credit Control Charging Credit behavior.

preemptively-request
Specifies RADIUS/Diameter prepaid credit preemptively requested charging credit behavior. If this option is used, a quota is requested for the specific type of content during the session initialization.

rating-group coupon_id
Specifies the coupon ID used in prepaid charging as rating-group which maps to the coupon ID for prepaid customer.

Important: This rating-group overrides the content ID, if present in the same charging-action for the prepaid customer in DCCA. But only the content IDs will be used in eG-CDRs irrespective of the presence of rating-group in that charging-action.

coupon_id must be an integer from 0 through 65535.
This option also assigns different content-types for the same charging action depending upon whether prepaid is enabled or not.

Usage

Use this command to configure RADIUS/Diameter Prepaid Credit Control Charging behavior.
This command selects reservation based credit control. A CCR-Initial is used to reserve quota upon the first traffic, then a series of CCR-updates are issued as the traffic proceeds and quota dwindles. A CCR-Terminate is issued at the end of the session or at the end of the quota-hold-time.
Example

cca charging credit
charge-units

This command configures the unit amount counters for RADIUS/DCCA charging calculation.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
charge-units units

{ default | no } charge-units
```

- **no**
  Disables the charge-units configuration.

- **default**
  Configures the default setting.
  Default: 0; disables the counter, same as `no charge-units`

- **units**
  Sets the service-specific fixed unit counter per content ID for RADIUS/DCCA charging.
  `units` is the value set for charging unit, and must be an integer from 1 through 65535.

**Usage**

This command configures the unit amount counters for charging calculation on per content ID basis for different protocols and packets regardless of packet direction (uplink or downlink).

**Important:** For more information on content ID, refer to the `if-protocol` command in the *Ruledef Configuration Mode Commands* chapter.

**Example**

The following command sets the charging unit to `1024`:

```plaintext
charge-unit 1024
```
charge-volume

This command configures how the volume amount counter for eG-CDR and DCCA charging are calculated.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
charge-volume { protocol { bytes | packet-length | packets } [ downlink | uplink ] | constant value }
{ no | default } charge-volume
```

**no**
Disables the charge-volume configuration.

**default**
Configures the default setting.
Default: `charge-volume ip bytes`

**protocol**
Specifies the charge volume method for the specific rule definition.
`protocol` must be one of the following:
- `dns`: Charge volume for DNS
- `ftp-control`: Charge volume for FTP-Control
- `ftp-data`: Charge volume for FTP-Data
- `http`: Charge volume for HTTP
- `icmp`: Charge volume for ICMP
- `imap`: Charge volume for Internet Message Access Protocol (IMAP)
- `ip`: Charge volume for IP
- `mms`: Charge volume for MMS
- `pop3`: Charge volume for POP3
- `rtp`: Charge volume for RTP
- `rtsp`: Charge volume for RTSP
- `sdp`: Charge volume for SDP
- `secure-http`: Charge volume for secure-https
- `sip`: Charge volume for SIP
- `smtp`: Charge volume for SMTP
- `tcp`: Charge volume for TCP
- **udp**: Charge volume for UDP
- **wsp**: Charge volume for WSP
- **wtp**: Charge volume for WTP

**bytes**
Sets charge volume for bytes.

**packet-length**
Sets charge volume for packet length.

**packets**
Sets charge volume for packets.

**constant units**
This sets the fixed increment value for charging. 
`units` is the value set for charging, and must be an integer from 0 through 65535.
If `constant` 3 is configured for every invocation of this Charging Action, the system adds 3 to the downlink/uplink volume counter, depending on the direction of packet.

**Usage**
This command provides the method for charging volume calculation for different protocols and packets. For information on supported protocols see the Ruledef Configuration Mode Commands chapter.
If `charge-volume rtp packets` is configured, system computes volume amounts for different options for RTP as follows:

<table>
<thead>
<tr>
<th>Volume</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume amount</td>
<td>Total (downlink and uplink) RTP packets</td>
</tr>
<tr>
<td>Volume amount uplink</td>
<td>Uplink RTP packets</td>
</tr>
<tr>
<td>Volume amount downlink</td>
<td>Downlink RTP packets</td>
</tr>
<tr>
<td>Volume amount uplink packets</td>
<td>Uplink RTP packets</td>
</tr>
<tr>
<td>Volume amount downlink packets</td>
<td>Downlink RTP packets</td>
</tr>
<tr>
<td>Volume amount uplink bytes</td>
<td>Uplink RTP bytes</td>
</tr>
<tr>
<td>Volume amount downlink bytes</td>
<td>Downlink RTP bytes</td>
</tr>
</tbody>
</table>

**Important**: Whenever service counts volume, it counts all packets that the relevant analyzers accepted.

**Important**: If a TCP packet is routed to the HTTP analyzer but there is no HTTP payload, then the TCP statistics will be updated but the HTTP statistics will not be updated (except for the “packets ignored by the HTTP analyzer” statistic).
Example
Following command sets the charging volume of downlink packets for RTP:

```
charge-volume rtp packets downlink
```
content-filtering processing server-group

This command enables/disables content filtering in the charging action.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

content-filtering processing server-group

{ default | no } content-filtering processing

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the default setting.</td>
</tr>
<tr>
<td>Default: content filtering configured for the rulebase is attempted</td>
</tr>
</tbody>
</table>

| no |
| Specifies to bypass content filtering. |
| This configuration should only be specified for charging actions that are performed when known safe sites are being accessed. |

Usage

Use this command to enable/disable content filtering in the charging action. This command works as second level filter to process the HTTP/WAP GET request with ICAP after ruledef matching. The first level filtering is in the rulebase configuration. This CLI command is only effective when the rulebase is configured with content-filtering mode server-group.

Example

The following command enables content filtering in the current charging action:

content-filtering processing server-group
content-id

This command specifies an optional content ID to use in the generated billing records, as well as the AVP used by the credit control application, such as the Rating-Group AVP for use by DCCA.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
content-id content_id
no content-id
```

- `no` Removes the content ID configuration from the charging action.

- `content_id`
  `content_id` is the content ID specified for credit control service in an active charging service, and must be an integer from 1 through 65535.

Usage
This command specifies an optional content ID to use in the generated billing records. This identifier assists the carrier’s billing post processing and also used by credit-control system to use independent quotas for different value of `content-id`.

If the specified Ruledef uses the `if-protocol` command to select a value for content ID, then the `content_id` specified through this command is not used for billing record generation.

**Important:** For more information on `content-id`, refer to the `if-protocol` command in the Ruledef Configuration Mode Commands chapter.

Example
The following command sets the content ID in the current charging action to 23:

```plaintext
content-id 23
```
end

This command returns the CLI prompt to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```bash
down
```

**Usage**
Use this command to change to the Exec mode.
exit

This command exits the Charging Action Configuration mode and returns to the Active Charging Service Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the Active Charging Service Configuration mode.
flow action

This command specifies the actions for packets that match a rule definition. This command also specifies action on packet and flow for Session Control functionality.

Product
All

Privilege
Security Administrator, Administrator

Syntax

flow action { conditional user-agent end-token end_token_name | discard [ downlink | uplink ] | random-drop interval interval_start to interval_end pkts-to-drop packet_min to packet_max | readdress [ server ip_address ] [ port port_number ] | terminate-flow | terminate-session }

no flow action

no
Disables the flow action configured in this charging action.

conditional user-agent end-token end_token_name
Conditionally redirects the HTTP packets matched to a configured user-agent to a specified URL. The user agent is configured using the redirect user-agent command in the Active Charging Service Configuration Mode.
end_token_name must be an alpha and/or numeric string of 1 through 32 characters in length, and is configured with this command to end the redirection condition.

discard [ downlink | uplink ]
Discards the packet associated with this charging action.
downlink: Discards only downlink packets.
uplink: Discards only uplink packets.

random-drop interval interval_start to interval_end pkts-to-drop packet_min to packet_max
Specifies random drop as a charging action to degrade voice quality.
interval_start to interval_end: Specifies the random drop interval, in seconds, at which the voice packets will be dropped. interval_start and interval_end must be integers from 1 through 999.
pkts-to-drop packet_min to packet_max: Specifies the number of voice packets to be dropped at a time in a flow when the packets have to be dropped. packet_min and packet_max must be integers from 1 through 100.

readdress { server ip_address [ port port_number ] | port port_number }
Specifies the re-address server’s IP address/port number for this charging action. Enables readdressing of packets based on the destination IP address in the packets.
ip_address must be the re-address server’s IP address, and must be an IPv4 address.
port_number must be the re-address server’s port number, and must be an integer from 1 through 65535.

**terminate-flow**

Specifies the flow action to terminate flow.
Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server. If the flow does not use TCP, this option simply discard the packets. This option is used for flows that use TCP only.

**terminate-session**

Specifies the flow action to terminate session.
When a rule pointing to a charging action configured with the terminate-session keyword is hit, then the corresponding session will be terminated.

**Usage**

Use this command to set the flow actions; e.g. discard, terminate, or conditional redirect.
When a re-address server is configured for a charging action, the show configuration command will show the readdress related configuration only if server address is configured. And the show configuration verbose command will show the readdress sever if configured, else will display “no flow action”.

**Example**

The following command sets the flow action to terminate:

```
flow-action terminate-flow
```
flow action redirect-url

This command specifies the redirection of URL for packets that matches a rule definition. This command also specifies the redirect-URL action on packet and flow for Session Control functionality.

Product
All

Privilege
Security Administrator, Administrator

Syntax

flow action redirect-url url/%3furl=dynamic_field [ clear-quota-retry-timer ]

{ default | no } flow action redirect-url

---

no
Disables the configured flow action in this charging action.

---

default
Disables the flow action and forward the packets normally.

---

redirect-url url/%3furl=dynamic_field

Redirects the HTTP packets matched to this Ruledef to the specified URL.
url must be a string size of from 1 through 511 characters in http://search.com/subtarg/%3furl=#HTTP.URL# format.
%3furl= specifies the delimiter ―?url=‖ between URLs.
Note that user cannot supply ―?‖ through CLI so %3f is the value for ―?‖.
dynamic_field indicates the dynamic fields for redirect URLs.
Dynamic fields must be enclosed in '#'. Up to 16 dynamic fields are allowed in the redirect string.
Allowed dynamic fields are:
• #BEARER.CALLED-STATION-ID#
• #BEARER.CALLING-STATION-ID#
• #BEARER.NAS-IP-ADDRESS#
• #BEARER.USER-NAME#
• #BEARER.ACCT-SESSION-ID#
• #BEARER.CORRELATION-ID#
• #BEARER.RULEBASE#
• #BEARER.SERVED-BSA-ADDR#
• #BEARER.SERVICE-NAME#
• #BEARER.SUBSCRIBER-ID#
• #BEARER.MSISDN#
• #HTTP.URL#
• #HTTP.URI#
Charging Action Configuration Mode Commands

flow action redirect-url

- #HTTP.HOST#
- #RTSP.URI#
- #WSP.URL#

**clear-quota-retry-timer**

This option resets the Credit Control Application quota retry timer for specific subscriber upon redirection.

**Usage**

Use this command to set the redirection of URL as flow actions upon matching of a Ruledef. This CLI can be used to redirect SIP requests as well. The following is a sample configuration:

```plaintext
configure

active-charging service s1

charging-action ca_sip_redir

content-id 10

flow action redirect-url sip:test@sip.org

exit

ruledef sip_req

sip request packet = TRUE

exit

rulebase plan1

action priority 08 ruledef sip_req charging-action ca_sip_redir

/* other rules, routing rules for sip, etc */

end
```

This would mean any SIP request that hits the *sip_req* ruledef, would get redirected to the url given in *ca_sip_redir*. This involves creating a redirection packet with the following response line and “Contact” header in the response.

SIP/2.0 302 Moved Temporarily
302 Moved Temporarily

Most of the header fields are copied directly from the request, so that the mandatory SIP headers are present. If content-length header was seen in the original message, it is replaced in the reply with ‘Content-Length: 0’.

**Example**

The following command resets quota retry timer upon redirection of flow to HTTP URL

```
flow action redirect-url http://search.com/%3url#http://msn.com#
clear-quota-retry-timer
```

flow action redirect-url
flow idle-timeout

This command configures the maximum duration a flow can remain idle after which the system automatically terminates the flow.

Product
All

Privilege
Security Administrator, Administrator

Syntax

flow idle-timeout idle_timeout

{ no | default } idle-timeout

- no
  Disables the idle-timeout configuration; sets the idle-timeout to 0 seconds.

- default
  Configures the default setting.
  Default: 300 seconds

  idle-timeout idle_timeout
  Specifies the maximum duration, in seconds, a flow can remain idle.
  idle_timeout must be an integer from 0 through 86400.

Usage

Use this command to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

Example

The following command configures the idle-timeout setting to 400 seconds:

  flow idle-timeout 400
flow limit-for-bandwidth

This command enables and configures bandwidth limits for Session Control functionality to the subscriber. Uplink and downlink limits are configured separately.

Product
All

Privilege
Security Administrator, Administrator

Syntax

flow limit-for-bandwidth { { direction { downlink | uplink } peak-data-rate bps peak-burst-size bytes violate-action { discard | lower-ip-precedence } [ committed-data-rate bps committed-burst-size bytes [ exceed-action { discard | lower-ip-precedence } ] ] ] | { id id } }

{ default | no } flow limit-for-bandwidth { direction { downlink | uplink } | id }

no
Disable bandwidth control traffic policing for the specified direction for the current subscriber.

default
Resets the bandwidth control policy to default mode.

direction { downlink | uplink }
Specifies the direction of flow downlink/uplink to apply bandwidth limit.
downlink: Flow of data towards subscriber.
uplink: Flow of data from subscriber.

peak-data-rate bps
Default: 256000
Specifies the peak data-rate for the subscriber, in bps (bits per second).
bps must be an integer from 1 through 4294967295.

peak burst-size bytes
Default: 3000
The peak burst size allowed, in bytes.
bytes must be an integer from 1 through 4294967295.

Important: It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.
### Charging Action Configuration Mode Commands

**flow limit-for-bandwidth**

---

```plaintext
violate-action { discard | lower-ip-precedence }
```

Default: Discard.

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **discard**: Discard the packet
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence

---

```plaintext
committed-data-rate bps
```

Default: 144000

The committed data rate (guaranteed-data-rate) in bps (bits per second).

*bps* must be an integer from 1 through 4294967295.

---

```plaintext
committed-burst-size bytes
```

Default: 3000

The committed burst size allowed, in bytes.

*bytes* must be an integer from 1 through 4294967295.

---

```plaintext
exceed-action { discard | lower-ip-precedence }
```

Default: lower-ip-precedence

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **discard**: Discard the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence

If exceed-action is not configured, the packets are forwarded.

---

```plaintext
id id
```

**Important**: This keyword is only available in StarOS 8.1 and later releases.

Specifies identifier for bandwidth limiting, and must be an integer from 1 through 65535.

This identifier enables traffic policing based on a separate identifier other than content ID. This identifier will always take priority over content ID. If this identifier is not configured, traffic policing will be based on content ID.

---

**Usage**

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions under Session Control.

**Important**: If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the `ip user-datagram-tos copy` command is configured to. In addition, the `lower-ip-precedence` option may also override the `ip qos-dscp` command configuration. Therefore, it is recommended that command not be used when specifying this option.

Details of the QoS Traffic Policing feature is available in the *System Enhanced Feature Configuration Guide*. 

---

*Cisco ASR 5000 Series Command Line Interface Reference*
Example
The following command sets an uplink peak data rate of 128000 bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth uplink peak-data-rate 128000 violate-action lower-ip-precedence
```

The following command sets a downlink peak data rate of 256000 bps and discards the packets when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth downlink peak-data-rate 256000 violate-action discard
```
flow limit-for-flow-type

This command controls the action in the event of number of flows exceeds for a type of flow under Session Control feature.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
flow limit-for-flow-type limit over-limit-action action_type
[ no ] limit-for-flow-type

no
Disables limit for the total number of flow for a type.

limit
Sets the maximum number of flows of a type exceeding which action triggers.
limit must be an integer from 1 through 400000000.

over-limit-action action_type
Triggers the action of action_type on exceeding limit for a flow type.
action_type must be one of the following:
discard: Discards the packets
direct-url: Redirects the flow
terminate-flow: Terminates the flow to which this packet belongs
terminate-session: Terminates the session to which this packet belongs
```

Usage

Use this command to control the action for the total number of flow of a type.

Example

The following command terminates the flow if total number of flows of a type exceeds 1024:
```
flow limit-for-flow-type 1024 over-limit-action terminate-flow
```
ip tos

This command sets the IP Type of Service (ToS) octets being used in the charging action.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |
af42 | af43 | be | ef | lower-bits tos_value } [ uplink | downlink ]
```

```
no ip tos [ uplink | downlink ]
```

no
Disables IP ToS being used in the charging action.

afxx
Specifies the use of an assured forwarding xX PHB.

be
Specifies the use of best effort forwarding PHB.

ef
Specifies the use of expedited forwarding PHB.

lower-bits tos_value

**Important:** In StarOS 8.1 and later releases, this keyword is **lower-bits tos_value**. In StarOS 8.0, it is **tos_value**.

Sets the least-significant 6 bits in the TOS byte with the specified numeric value. **tos_value** must be an integer from 0 through 63.

downlink
Specifies the ToS for downlink packets only.

uplink
Specifies the ToS for uplink packets only.

Usage
Use this command to set the IP Type of Service (ToS) octets used in the charging action. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the TOS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the TOS byte.

Example
The following command sets the IP ToS to be with downlink:

```bash
ip tos be downlink
```
ip vlan

This command configures the VLAN identifier to be associated with the IP address for the session.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip vlan range
{ default | no } ip vlan
```

```
default | no
These options delete or disable the IP VLAN configuration.

range
range must be an integer from 1 through 4094.
```

Usage
This command configures the subscriber VLAN ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, then this subscriber configured VLAN ID overrides it. Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

Example
The following command sets the IP VLAN range to go up to 500:

```
ip vlan 500
```

The following command sets the IP VLAN range back to default.

```
default ip vlan
```
nexthop-forwarding-address

This command configures the next-hop forwarding address for this charging action.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
no nexthop-forwarding-address
```

```
nexthop-forwarding-address  ipv4_address
```

```
no
```

Removes the next-hop forwarding address, if previously configured.

```
ipv4_address
```

`ipv4_address` must be the next-hop forwarding address for this charging action, and must be specified using the standard IPv4 dotted decimal notation.

Usage
Use this command to configure the next-hop forwarding address for a charging action. When an uplink packet matches a rule and a charging action is applied to it this next-hop forwarding address is used. There are different methods to configure a next-hop forwarding address, they are prioritized as follows:

- the next-hop forwarding address, if configured, in a redirect ACL is used
- else, the next-hop address configured in the charging action is used
- else, the next-hop address, if configured, in the IP pool is used

Example
The following command sets the next-hop forwarding address for the current charging action to `1.1.1.1`:

```
nexthop-forwarding-address 1.1.1.1
```
qos-class-identifier

This command sets the QoS Class Identifier.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
qos-class-identifier identifier

no qos-class-identifier
```

- **no**
  - Removes QoS Class Identifier, if previously configured.

- **identifier**
  - Specifies the QoS Class Identifier, and must be an integer from 1 through 9.

**Usage**

Use this command to set the QoS Class Identifier.

**Example**

The following command sets the QoS Class Identifier as 3:

```
qos-class-identifier 3
```
qos-renegotiate

This command configures the QoS traffic class for the charging action for the Layer 7 QoS Renegotiation feature, enabling triggering QoS renegotiation from an active-charging rule.

**Important:** This command is controlled by the dynamic-qos-renegotiation license.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
qos-renegotiate traffic-class { background | conversational | interactive
priority | streaming }
```

```
no qos-renegotiate
```

- **no**
  Removes any previously configured traffic class setting.

- **background**
  Specifies the traffic class as Background.
  For traffic patterns in which the data transfer is not time-critical (for example e-mail exchange).

- **conversational**
  Specifies the traffic class as Conversational.
  For traffic patterns in which there is a constant flow of packets.

- **interactive priority**
  Specifies the traffic class as Interactive.
  For traffic patterns in which there is an intermittent flow of packets.
  `priority` specifies the traffic handling priority, and must be an integer from 1 through 3.

- **streaming**
  Specifies the traffic class as Streaming.
  For traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.

**Usage**

Use this command to configure the QoS traffic class for a charging action for the Layer 7 QoS Renegotiation feature, enabling triggering QoS renegotiation from an active-charging rule.

Layer 7 QoS Renegotiation is an extension of the Dynamic QoS Renegotiation feature. Upon matching a particular layer 7 rule, for example the access of a particular URL, the GGSN triggers the renegotiation of the PDP context.
Example
The following command sets the QoS traffic class for the charging action to streaming:

```
qos-renegotiate traffic-class streaming
```
retransmissions-counted

This command enables the charging action to count the number of retransmissions.

Product: All

Privilege: Security Administrator, Administrator

Syntax

[ no | default ] retransmissions-counted

no | default
Disables the count retries from the charging action.

Usage

Use this command to enable counting of the number of retransmissions.

Example

retransmissions-counted
service-identifier

This command configures the service identifier for a service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
service-identifier service_id

no service-identifier
```

Usage
Use this command to configure the service identifier for a service.

Example
The following command sets the service identifier for a service as 99:
```
service-identifier 99
```
tft packet-filter

This command configures the packet filter to be sent to the MS.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] tft packet-filter packet_filter_name
```

- **no**
  - Removes the specified packet filter, if previously configured.

- **packet_filter_name**
  - `packet_filter_name` specifies the packet filter’s name, and must be a string of 1 through 63 characters in length.

Usage

Use this command to configure the packet filter to be sent to the MS. Up to eight packet filters can be specified in a charging action.

Example

The following command configures the packet filter `filter23` to be sent to the MS:

```
tft packet-filter filter23
```
tos

This command sets the Type of Service (ToS) octets used in the charging action.

Product
All

Privilege
Security Administrator, Administrator

Syntax

tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | be | ef | lower-bits tos_value } [ downlink | uplink ]

no tos [ downlink | uplink ]

no
Disables the ToS being used in the charging action.

afxx
Specifies the use of an assured forwarding \textit{xx} Per Hop Behavior (PHB).

be
Specifies use of Best Effort forwarding PHB.

ef
Specifies use of Expedited Forwarding PHB.

lower-bits tos_value

\textbf{Important:} In StarOS 8.1 and later releases, this keyword is \textit{lower-bits tos_value}. In StarOS 8.0, it is \textit{tos_value}.

Sets the least-significant 6 bits in the TOS byte with the specified numeric value. value must be an integer from 0 through 63.

downlink
Specifies the ToS only for downlink packets.

uplink
Specifies the ToS only for uplink packets.

Usage
Use this command to set the ToS octets used in the charging action. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the TOS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the TOS byte.

Example
The following command sets the ToS to be for downlink packets:

```
tos be downlink
```
xheader-insert

This command specifies the extension-header (x-header) format name whose fields are to be inserted in HTTP GET and POST request packets.

**Important**: This command is license dependent. For more information please contact your local sales representative.

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax**

```
xheader-insert xheader-format xheader_format_name [ first-request-only ] [ -noconfirm ]
```

**no xheader-insert**

```
no
```

Removes previously configured x-header format name.

```
xheader-format format_name
```

Enables x-header mode configuration, and specifies name of the x-header format whose fields are to be inserted in the packets.

- `format_name` must be a string of 1 through 63 characters in length.

```
first-request-only
```

Specifies x-header insertion only for the first HTTP request in the IP flow. If not configured, the default behavior is insertion for all requests.

```
-noconfirm
```

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

**Usage**

Use this command to enable x-header mode, and specify the x-header format name whose fields are to be inserted in HTTP GET and POST request packets.

Also, see **xheader-format CLI command** in the *Active Charging Service Configuration Mode* and the *x-header Format Configuration Mode Commands* chapters.

**Example**

The following command enables x-header mode, and specifies the x-header format name as `test12`:

```
xheader-insert xheader-format test12
```
Class-Map is used to configure a packet classifier for flow-based Traffic Policing feature within destination context. It filters egress and/or ingress packets of a subscriber session based on rules configured in a subscriber context.

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the context configuration mode and returns to the global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the global configuration mode.
match any

This command allows all traffics in this class map.

**Product**
PDSN, HA, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match any
```

**Usage**
Sets the match rule to allow all traffic flow for specific class map.

**Example**
The following commands allows all packets going to a system with this class map.

```
match any
```
match dst-ip-address

This command specifies a traffic classification rule based on the destination IP address of packets.

Product
PDSN, HA, ASN-GW

Privilege
Security Administrator, Administrator

Syntax
match dst-ip-address dst_ip_address subnet_mask

dst_ip_address
Specifies the destination IP address of the packets. dst_ip_address must be specified using the standard IPv4 dotted decimal notation.

subnet_mask
Specifies the IP address mask bits to determine the number of IP addresses in the pool. ip_mask must be specified using the standard IPv4 dotted decimal notation.
1 bits in the ip_mask indicate that bit position in the ip_address must also have a value of 1.
0 bits in the ip_mask indicate that bit position in the ip_address does not need to match, i.e., the bit can be either a 0 or a 1.
For example, if the IP address and mask are specified as 172.168.10.0 and 255.255.255.224, respectively, the pool will contain IP addresses in the range 172.168.10.0 through 172.168.10.31 for a total of 32 addresses.

Usage
Sets the match rule based on the destination IP address of packets for specific Class Map.

Example
The following commands specifies the rule for packets going to a system having an IP address 10.1.2.6.
machine dst-ip-address 10.1.2.6
match dst-port-range

This command specifies a traffic classification rule based on the range of destination ports of L4 packets.

**Product**

PDSN, HA, ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
match dst-port-range initial_port_number [ to last_port_number ]
```

Specifies the destination port or range of ports of L4 packets.
- `initial_port_number` is the starting port number and must be an integer value in the range from 1 through 65535 but less than `last_port_number`, if specified.
- `last_port_number` is the end port number and must be an integer value in the range from 1 through 65535 but more than `initial_port_number`.

**Usage**

Sets the match rule based on the destination port number or range of ports of L4 packets for specific Class Map.

**Example**

The following commands specifies the rule for packets having destination port number from 23 to 88.

```
match dst-port-range 23 to 88
```
match ip-tos

This command specifies a traffic classification rule based on the IP Type of Service value in ToS field of packet.

**Syntax**

```plaintext
match ip-tos { service_value [ ip-tos-mask mask_value ] | tos-range low_value to high_value }
```

- **service_value**
  - Specifies the IP Type-of-Service value to match inside the ToS field of packets.
  - `service_value` must be an integer value in the range from 0 through 255.
- **ip-tos-mask mask_value**
  - Specifies the IP Type-of-Service mask value to match inside the ToS field of packets.
  - `mask_value` must be an integer value in the range from 1 through 255.
- **tos-range low_value to high_value**
  - Specifies a range that a ToS value in a received packet must fall within to be considered a match.
  - `low_value` and `high_value` must be an integer from 0 to 255.

**Usage**

Sets the match rule based on the IP ToS value in ToS field of packets for specific Class Map.

**Example**

The following commands specifies the IP ToS value of 3 is the value to match in a ToS field in received packets.

```plaintext
match ip-tos 3
```
match ipsec-spi

This command specifies a traffic classification rule based on the IPSec Security Parameter Index (SPI) value in SPI field of packet.

**Product**
PDSN, HA, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match ipsec-spi index_value
```

*index_value*

Specifies the IPSec SPI value to match inside the SPI field of packets.

*index_value* must be an integer value in the range from 1 through 65535

**Usage**
Sets the match rule based on the IPSec SPI value in SPI field of packets for specific Class Map.

**Example**
The following commands specifies the IPsec SPI value to 1234 for SPI field in packets

```
match ipsec-spi 1234
```
match packet-size

This command specifies a traffic classification rule based on the size of packet.

**Product**
PDSN, HA, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match packet-size [ gt | lt ] size
```

- `size`
  Specifies the packet length in bytes.
  `length` must be an integer value in the range from 1 through 65535.

- `[ gt | lt ]`
  Applies operator to specify a range of packets having packet size greater than or less than the specified size `size`.

**Usage**
Sets the match rule based on the size of packets for specific Class Map. This command is only applicable for static policies; it is not available for dynamic policies.

**Example**
The following commands specifies the packet length to 1024 bytes.

```
match packet-size 1024
```
**match protocol**

This command specifies a traffic classification rule based on the protocol used for session flow.

**Product**

PDSN, HA, ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
match protocol { tcp | udp | gre | ip-in-ip }
```

---

**tcp**

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the protocol field to tcp inside the packet.

---

**udp**

Sets the match rule for a session flow having User Datagram Protocol (UDP). It matches the protocol field to udp inside the packet.

---

**gre**

Sets the match rule for session flow using Generic Routing Encapsulation (GRE) Protocol. It matches the protocol field to gre inside the packet.

---

**ip-in-ip**

Sets the match rule for session flow using IP-in-IP encapsulation protocol. It matches the protocol field to ip-in-ip inside the packet.

---

**Usage**

Sets the match rule based on the protocol of packet flow for a specific Class Map.

---

**Example**

The following commands specifies the rule for packet flow using IP-in-IP as protocol.

```
match protocol ip-in-ip
```
**match src-ip-address**

This command specifies a traffic classification rule based on the source IP address of packets.

**Product**

PDSN, HA, ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
match src-ip-address src_ip_address subnet_mask
```

```
src_ip_address
Specifies the source IP address of the packets.

subnet_mask
Specifies the IP address mask bits to determine the number of IP addresses in the pool. ip_mask must be specified using the standard IPv4 dotted decimal notation.

1 bits in the ip_mask indicate that bit position in the ip_address must also have a value of 1.

0 bits in the ip_mask indicate that bit position in the ip_address does not need to match, i.e., the bit can be either a 0 or a 1.

For example, if the IP address and mask are specified as 172.168.10.0 and 255.255.255.224, respectively, the pool will contain IP addresses in the range 172.168.10.0 through 172.168.10.31 for a total of 32 addresses.
```

**Usage**

Sets the match rule based on the source IP address of packets for specific Class Map.

**Example**

The following commands specifies the rule for packets coming from a system having an IP address 10.1.2.3.

```
match src-ip-address 10.1.2.3
```
match src-port-range

This command specifies a traffic classification rule based on the range of source ports of L4 packets.

Product
PDSN, HA, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```
match src-port-range initial_port_number [ to last_port_number ]
```

`initial_port_number` [ to `last_port_number` ]

Specifies the source port or range of ports of the L4 packets.
`initial_port_number` is the starting port number and must be an integer value in the range from 1 through 65535 but less than `last_port_number`, if specified.
`last_port_number` is the end port number and must be an integer value in the range from 1 through 65535 but more than `initial_port_number`.

Usage
Sets the match rule based on source port number or range of ports of L4 packets for specific Class Map.

Example
The following commands specifies the rule for packets having source port number from 23 to 88.

```
match src-port-range 23 to 88
```
Chapter 35
Content Filtering Policy Configuration Mode Commands

In the Content Filtering Policy (CFP) Configuration Mode, you can configure analysis and action on matching results of content filtering analysis for Content Filtering Category Policy Identifier.

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

This command specifies the action to take for the indicated result after content filtering analysis.

Product CF

Privilege Security Administrator, Administrator

Syntax

```
analyze priority priority { all | category category | x-category string } action { allow | content-insert content_string | discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ edr edr_format_name ]
```

```
no analyze priority priority
```

```
no
Removes the specified analyze priority configuration.
```

```
priority priority
Specifies the precedence of a category in the content filtering policy.
priority must be an integer from 1 through 65535, and must be unique in the content filtering policy.
```

```
all
Specifies the default action to take if the category returned after rating is not configured in the subscriber’s content filtering policy. This has the lowest priority.
```

```
category category
Specifies the category. category must be one of the following.
```

```
Important: Content can simultaneously match multiple categories, therefore specific priority must be used for required evaluation precedence.
```

<table>
<thead>
<tr>
<th>• ABOR</th>
<th>• ADULT</th>
<th>• ADVERT</th>
<th>• ANON</th>
<th>• ART</th>
</tr>
</thead>
<tbody>
<tr>
<td>• AUTO</td>
<td>• BLACK</td>
<td>• BLOG</td>
<td>• BUSI</td>
<td>• CAR</td>
</tr>
<tr>
<td>• CHAT</td>
<td>• CMC</td>
<td>• CRIME</td>
<td>• CULT</td>
<td>• DRUG</td>
</tr>
<tr>
<td>• DYNAM</td>
<td>• EDU</td>
<td>• ENERGY</td>
<td>• ENT</td>
<td>• FIN</td>
</tr>
<tr>
<td>• FORUM</td>
<td>• GAMB</td>
<td>• GAME</td>
<td>• GLAM</td>
<td>• GOVERN</td>
</tr>
<tr>
<td>• HACK</td>
<td>• HATE</td>
<td>• HEALTH</td>
<td>• HOBBY</td>
<td>• HOSTS</td>
</tr>
</tbody>
</table>
**Content Filtering Policy Configuration Mode Commands**

<table>
<thead>
<tr>
<th>• KIDS</th>
<th>• LEGAL</th>
<th>• LIFES</th>
<th>• MAIL</th>
<th>• MIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>• NEWS</td>
<td>• OCCULT</td>
<td>• PEER</td>
<td>• PERS</td>
<td>• POLTIC</td>
</tr>
<tr>
<td>• PORN</td>
<td>• PORTAL</td>
<td>• PROXY</td>
<td>• REF</td>
<td>• REL</td>
</tr>
<tr>
<td>• SCI</td>
<td>• SEARCH</td>
<td>• SHOP</td>
<td>• SPORT</td>
<td>• STREAM</td>
</tr>
<tr>
<td>• SUIC</td>
<td>• SXED</td>
<td>• TECH</td>
<td>• TRAV</td>
<td>• VIOL</td>
</tr>
<tr>
<td>• VOIP</td>
<td>• WEAP</td>
<td>• WHITE</td>
<td>• UNKNOWN</td>
<td></td>
</tr>
</tbody>
</table>

**x-category string**

This keyword can be used to configure runtime categories not present in the CLI. 
*string* specifies the unclassified category to be rated, and must be an alpha and/or numeric string of 1 through 6 characters in length. 
A maximum of 10 x-categories can be configured.

**action { allow | content-insert content_string | discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code }**

Specifies the action to take for the indicated result of content filtering analysis. 
*allow*: In the case of static content filtering this option allows the request for content, and in dynamic content filtering allows the content itself. 
*content-insert content_string*: Specifies the content string to be inserted in place of the message returned from prohibited/restricted site or content server. 
In case of static content filtering, *content_string* is used to create a response to the subscriber’s attempt to get content, and in dynamic content filtering, it is used to replace the content returned by a server. 
*discard*: in case of static content filtering this option discards the packet(s) that requested, and in dynamic content filtering it discards the packet(s) that contain(s) the content. 
*redirect-url url*: Specifies redirecting the subscriber to the specified URL. 
*url* must be a string of 1 through 1023 characters in length, and in the http://search.com/subtarg=#HTTP.URL# format. 
*terminate-flow*: Specifies terminating the TCP connection gracefully between the subscriber and server, and sends a TCP FIN to the subscriber and a TCP RST to the server. 
*www-reply-code-and-terminate-flow reply_code*: Specifies terminating flow with the specified reply code. *reply_code* must be a reply code, and must be an integer from 100 through 599.

**Important:** Static-and-Dynamic Content Filtering is only supported in StarOS 9.0 and later.

**edr edr_format_name**

Specifies to generate separate EDRs for content filtering based on action and content category using EDR file format name *edr_format_name*. 
*edr_format_name* is the name of a pre-defined EDR file format name in the EDR Format Configuration Mode, and must be an alpha and/or numeric string of 1 through 63 characters in length.

---

**Cisco ASR 5000 Series Command Line Interface Reference**

OL-22948-01

---
**Important:** EDRs generated through this keyword are different from charging EDRs generated for subscriber accounting and billing. For more information on generation of charging EDRs, refer to the *Rulebase Configuration Mode Commands* chapter.

**Usage**

Use this command to specify the action and priorities for the indicated result of content filtering analysis. Up to 64 priorities and actions can be entered with this command.

**Example**

The following command sets priority 10 for category *ADULT* with action as *terminate-flow*:

```plaintext
analyze priority 10 category ADULT action terminate-flow
```
discarded-flow-content-id

This command is used in the configuration to account for packets discarded as a result of content filtering action.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

```
discarded-flow-content-id content_id

no discarded-flow-content-id
```

```
content_id

Specifies content ID for discarded flows.
content_id must be an integer from 1 through 65535.
```

Usage

Use this command in the configuration to account for packets discarded as a result of CF action.

A flow end-condition EDR would be generated as a charging EDR for content-filtered packets. No billing EDRs (even with flow-end) would be generated for a discarded packet as the flow will not end. Dual EDRs would exist for customers who want to use “flow end” to get EDRs for charging, plus CF-specific EDRs. The second EDR for charging comes from the flow end-condition content-filtering configuration in the Rulebase Configuration Mode.

The discarded-flow-content-id configuration can be used for accumulating stats for UDR generation in case CF discards the packets. These stats for UDR generation (based on the CF content ID) would also be accumulated in case of ACS error scenarios where the packets are discarded but the flow does not end.

If, in the Rulebase Configuration Mode, the content-filtering flow-any-error configuration is set to deny, then all the denied packets will be accounted for by the discarded-flow-content-id config. I.e. the content_id will be used to generate UDRs for the denied packets in case of content filtering.

Example

Use the following command to set the accumulation of stats for UDR generation based on the CF content ID 1003:

```
discarded-flow-content-id 1003
```
failure-action

This command specifies the failure action when the content filtering analysis results are not available to analyze.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
failure-action { allow | content-insert content_string | discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ edr edr_format_name ]
```

**default failure-action [ edr edr_format_name ]**

- **default**
  Configures the default setting.
  Default: discard

- **allow**
  In static content filtering, this option allows the request for content, and in dynamic content filtering allows the content itself.

  **Important:** Static-and-Dynamic Content Filtering is only supported in StarOS 9.0 and later.

- **content-insert content_string**
  Specifies the content string to be inserted in place of the message returned from the content server due to connection timeout or when no category policy ID is available for the content.
  In case of static content filtering, the `content_string` is used to create a response to the subscriber’s attempt to get content, and in dynamic content filtering it replaces the content returned by a server.
  `content_string` must be an alpha and/or numeric string of 1 through 1023 characters in length.

  **Important:** Static-and-Dynamic Content Filtering is only supported in StarOS 9.0 and later.

- **discard**
  In static content filtering, specifies discarding the packet(s) that requested, and in dynamic content filtering discards the packet(s) that contain the content.

  **Important:** Static-and-Dynamic Content Filtering is only supported in StarOS 9.0 and later.

- **redirect-url url**
  Redirects the subscriber to the specified URL.
  `url` must be a string of 1 through 1023 characters in length, and must be in the following format:
http://search.com/subtarg=#HTTP.URL#

**terminate-flow**
Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server.

**www-reply-code-and-terminate-flow** *reply_code*
Sets action as terminate-flow with specified reply code.
*reply_code* must be a reply code, and must be an integer from 100 through 599.

**edr** *edr_format_name*
Specifies name of the EDR format to be generated on the content filtering action using EDR file format name *edr_format_name*.
*edr_format_name* is the name of a pre-defined EDR file format name in the EDR Format Configuration Mode, and must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**
Use this command to set the failure action to take when no content filtering analysis result is available to analyze for `analyze priority priority category category_string` command.

**Example**
The following command sets the failure action as `discard`:
`failure-action discard`
timeout action

This command has been deprecated, and is replaced by the `failure-action` command.
Chapter 36
Content Filtering Server Group Configuration Mode Commands

Content Filtering Server Group (CFSG) Configuration Mode is accessed by entering the content-filtering server-group command in the Context Configuration Mode.

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

This command configures the TCP connection retry timer for Internet Content Adaptation Protocol (ICAP) server and client.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
connection retry-timeout duration
{ default | no } connection retry-timeout
```

**default**
Configures the default setting.
Default: 30 seconds

**no**
Removes the connection retry timeout configuration.

**duration**
`duration` is the duration in seconds, and must be an integer from 1 through 3600.

**Usage**
Use this command to configure the connection retry timer between ICAP server and client TCP connection, i.e. how long to wait before reattempting to establish a TCP connection.

**Example**
The following command sets the ICAP client and server connection retry timer to 120 seconds.

```
connection retry-timeout 120
```
deny-message

This command configures the text message that is returned to the subscriber in a deny response.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

`deny-message string`

{ default | no } deny-message

---

**default**
Configures the default setting.
Default: Disabled

---

**no**
Removes previously configured deny message setting.

---

**string**
Specifies a text message that is to be returned to the subscriber in a deny response.
string must be an alpha and/or numeric string of 1 through 511 characters in length.

---

**Usage**
Use this command to define a text message that is returned to the subscriber in a deny response.

---

**Example**
The following command sets the text message to no_Authorization in a deny message:

```
deny-message no_Authorization
```
**dictionary**

This command specifies the dictionary to use for requests to the server(s) in this CFSG.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dictionary { custom1 | custom2 | standard }

{ default | no } dictionary
```

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Sets the default dictionary. Default: standard</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Removes the previously configured dictionary setting.</td>
</tr>
<tr>
<td><strong>custom1</strong></td>
<td>Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99. It provides proprietary header fields for MSISDN and APN/subscriber. Please contact your local sales representative for additional information.</td>
</tr>
<tr>
<td><strong>custom2</strong></td>
<td>Custom-defined dictionary. Please contact your local sales representative for additional information.</td>
</tr>
<tr>
<td><strong>standard</strong></td>
<td>Default: Enabled. This dictionary is used to use an HTTP Get Request to specify the URL. It is conforming to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to specify the standard and customized encoding mechanism used for elements included messages.

**Example**
The following command configures the system to use standard dictionary to encode messages:

```
default dictionary
```
end

Returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
failure-action

This command specifies the actions to be taken when communication between ICAP endpoints within this CFSG fail.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

failure-action { allow | content-insertion content_string | discard | redirect-url url | terminate-flow }

{ default | no } failure-action

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures the default setting. Default: <strong>terminate-flow</strong></td>
</tr>
<tr>
<td>no</td>
<td>Removes previously configured failure action.</td>
</tr>
<tr>
<td>allow</td>
<td>In case of static content filtering this option allows the request for content, and for dynamic content filtering it allows the content itself.</td>
</tr>
<tr>
<td>content-insertion content_string</td>
<td>Specifies the content string to be used for failure action. In case of static content filtering, the specified text <code>content_string</code> is used to create a response to the subscriber’s attempt to get content. In dynamic content filtering, the specified text <code>content_string</code> is used to replace the content returned by a server. <code>content_string</code> must be an alpha and/or numeric string of 1 through 128 characters in length.</td>
</tr>
<tr>
<td>discard</td>
<td>In case of static content filtering this option discards the packet(s) requested, and for dynamic content filtering it discards the packet(s) that contain(s) the content.</td>
</tr>
<tr>
<td>redirect-url url</td>
<td>Redirects the subscriber to the specified URL. <code>url</code> must be a string of 1 through 128 characters in length, and must be in the following format: <code>http://search.com/subtarg=#HTTP.URL#</code></td>
</tr>
<tr>
<td>terminate-flow</td>
<td>For TCP, gracefully terminates the connection between the subscriber and external server, and sends a TCP FIN to the subscriber and a TCP RST to the server.</td>
</tr>
</tbody>
</table>
For WAP-Connection Oriented, the WSP session is gracefully terminated by sending WTP Aborts for each of the outstanding requests, and WSP Disconnect to the client and the server. For WSP-Connectionless only the current WSP request is rejected.

**Usage**

Use this command to set the actions on failure for server connection.

ICAP rating is enabled for retransmitted packet when default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios. In these cases the retransmitted packet in the uplink direction is sent for ICAP rating again.

In case of WAP CO, uplink retransmitted packet for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request) then uplink retransmitted packet for each of the transaction is sent for rating again.

In case of HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken is sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP request for the same flow (pipelined request) then for the retransmitted packet the URL that will be sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on re-transmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- **WSP CO:**
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: The retransmitted packet is not sent for ICAP rating.
  - Redirect: The retransmitted packet is not sent for ICAP rating.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
  - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.

- **HTTP:**
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: Retransmitted packets are dropped and not charged.
  - Redirect: Retransmitted packets are dropped and not charged.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
  - Terminate flow: Retransmitted packets will be dropped and not charged.
Example
The following command sets the failure action to terminate:

```plaintext
failure-action terminate-flow
```
icap server

This command adds an Internet Content Adaptation Protocol (ICAP) server configuration to the current Content Filtering Server Group.

**Important:** In StarOS 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In StarOS 8.0 and earlier releases, only one ICAP Server can be configured per Content Filtering Server Group.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
icap server ip_address [ port port_number ] [ max msgs ] [ priority priority ]
no icap server ip_address [ port port_number ] [ priority priority ]
```

- `no`
  - Removes the specified ICAP server configuration from the current Content Filtering Server Group.

- `ip_address`
  - Specifies the ICAP server’s IP address.
  - `ip_address` must be a standard IPv4 address expressed in dotted decimal notation format, or an IPv6 address expressed in colon notation format.

- `port port_number`
  - Default: 1344
  - Specifies the ICAP server’s port number to use for communications.
  - `port_number` must be an integer from 1 through 65535.

- `max msgs`
  - Specifies the maximum number of unanswered outstanding messages that may be allowed to the ICAP server.

**Important:** The maximum outstanding requests per ICAP connection is limited to one. Therefore the value configured using the `max` keyword will be ignored.

- `priority priority`
  - Default: 1
  - Specifies priority of the ICAP server in the current Content Filtering Server Group. The priority is used in server selection to determine which standby server becomes active.
priority must be an integer from 1 through 65535, where 1 is the highest priority.

Important: The priority keyword is only available in StarOS 8.1 and later.

Usage
This command is used to add an ICAP server configuration to a Content Filtering Server Group with which the system is to communicate for content filtering communication.
In StarOS 8.0, the ICAP solution supports only one connection between ACS Manager and ICAP server.
In StarOS 8.1, multiple ICAP server connections are supported per manager. At any time only one connection is active with the other connections acting as standby. In case of a connection failure, based on its priority, a standby connection becomes active. Any pending ICAP requests are moved to the new active connection. If a standby connection is unavailable, failure action is taken on all pending ICAP requests. See the failure-action command.
In StarOS 8.1 and later, a maximum of five ICAP servers can be configured per Content Filtering Server Group with a priority associated with each server. Once configured, an ICAP server’s priority cannot be changed. To change a server’s priority, the server configuration must be removed, and added with the new priority.

Example
The following command sets the ICAP server IP address to 1.2.3.4 and port to 1024:
icap server 1.2.3.4 port 1024
The following command specifies an ICAP server with IP address 5.6.7.8, port number 1024, and priority 3:
icap server 5.6.7.8 port 1024 priority 3
origin address

This command specifies a bind address for the CFSG endpoint.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

```
origin address ip_address

no origin address
```

Usage
Use this command to set the bind address for the CFSG endpoint.

Example
The following command sets the origin address of 1.1.1.1:

```
origin address 1.1.1.1
```
response-timeout

This command sets the response timeout for the ICAP connection between ICAP server and client.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
response-timeout duration
{ default | no } response-timeout
```

- **default**
  Configures the default setting.
  Default: 30 seconds

- **no**
  Removes the response timeout configuration.

- **duration**
  Default: 30 seconds
  This is the timeout duration in seconds, and must be an integer from 1 through 300.

**Usage**

Use this command to set the ICAP connection response timeout, after which connection will be marked as unsuccessful between ICAP endpoint.

**Example**

The following command sets the ICAP connection response timeout to 100 seconds:

```plaintext
response-timeout 100
```
timeout action

This command has been deprecated, and is replaced by the failure-action command.
url-extraction

This command enables configuration of ICAP URL extraction behavior.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

url-extraction { after-parsing | raw }

default url-extraction

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the default setting.</td>
</tr>
<tr>
<td>Default: <strong>after-parsing</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>after-parsing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies sending parsed URI and host name. Percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters and sent.</td>
</tr>
<tr>
<td>For example, the URL:</td>
</tr>
<tr>
<td><code>http://www.google.co.uk/?this%20is%20a%20test</code></td>
</tr>
<tr>
<td>will be sent to the ICAP server as:</td>
</tr>
<tr>
<td><code>http://www.google.co.uk/?this is a test</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>raw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies sending raw URI and host name. The URLs will contain percent-encoded hex characters as is.</td>
</tr>
<tr>
<td>For example, the URL:</td>
</tr>
<tr>
<td><code>http://www.google.co.uk/?this%20is%20a%20test</code></td>
</tr>
<tr>
<td>will be sent to the ICAP server as:</td>
</tr>
<tr>
<td><code>http://www.google.co.uk/?this%20is%20a%20test</code></td>
</tr>
</tbody>
</table>

Usage

Use this command to configure the ICAP URL extraction behavior. Percent-encoded hex characters—for example, space (%20) and the percent character (%25)—in URLs sent from the ACF client to the ICAP server can be sent either as percent-encoded hex characters or as their corresponding ASCII characters.

Example

The following command configures URLs sent from the ACF client to the ICAP server to contain the escape encoding as is:

**url-extraction raw**
Chapter 37
Context Configuration Mode Commands

The Context Configuration Mode is used to create and manage the contexts within the system. Contexts facilitate management of subscribers and services within a system.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode
```
aaa accounting

This command enables/disables accounting for subscribers and context-level administrative users for the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

`aaa accounting { administrator radius-diameter | subscriber [ radius-diameter ] }`

default aaa accounting { administrator | subscriber }

`no aaa accounting { administrator | subscriber } [ radius-diameter ]`

default
Configures the default setting.
Default: RADIUS

no
Disables AAA accounting per the options specified.

administrator | subscriber
administrator: Enables/disables AAA accounting for context-level administrative users.
subscriber: Enables/disables AAA accounting for subscribers.

radius-diameter
Enables/disables RADIUS or Diameter accounting for administrator(s)/subscribers as specified.

Usage
Use this command to enable/disable accounting for subscribers and context-level administrative users for the current context.
To enable or disable accounting for individual local subscriber configurations refer to the `accounting-mode` command in the Subscriber Configuration Mode Commands chapter.

Important: The accounting parameters in the APN Configuration Mode take precedence over this command for subscriber sessions. Therefore, if accounting is disabled using this command but enabled within the APN configuration, accounting is performed for subscriber sessions.

Example
The following command disables AAA accounting for context-level administrative users:
no aaa accounting administrator
The following command enables AAA accounting for context-level administrative users:

aaa accounting administrator radius-diameter
aaa authentication

This command enables/disables authentication for subscribers and context-level administrative users for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

[ no ] aaa authentication { administrator | subscriber } { local | none | radius-diameter }

default aaa authentication { administrator | subscriber }

- **default**
  Configures the default setting.

- **administrator**
  Configures default administrator authentication (local+RADIUS).

- **subscriber**
  Configures AAA authentication for subscriber(s). This sets the default value, which is RADIUS.

- **no**
  Disables AAA authentication for administrator(s)/subscribers as specified.

- **local**
  Disables local authentication for current context.

- **radius-diameter**
  Disables RADIUS or Diameter-based authentication.

- **administrator | subscriber**

  - **administrator**
    Enables/disables authentication for administrative users.

  - **subscriber**
    Enables/disables authentication for subscribers.

- **local | none | radius-diameter**

  Enables AAA authentication for administrator(s)/subscribers as specified.

  - **local**
    Enables local authentication for current context.

  - **none**
    Disables authentication for current context.

  - **radius-diameter**
    Enables RADIUS or Diameter-based authentication.

**Usage**

Use this command to enable/disable AAA authentication during specific maintenance activities or during test periods. The authentication can then be enabled again for the entire context as needed.

**Example**

The following command disables RADIUS or Diameter-based authentication for subscribers for the current context:

```plaintext
no aaa authentication subscriber radius-diameter
```

The following command enables RADIUS or Diameter-based authentication for subscribers for the current context:
aaa authentication subscriber radius-diameter
aaa constructed-nai

Configures the password used during authentication for sessions using a constructed network access identifier (NAI) or an APN-specified user name.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
aaa constructed-nai authentication [ [ encrypted ] password user_password ]

no aaa constructed-nai authentication
```

- **no**
  - Disables authentication based upon the constructed network access identifier.

- **encrypted**
  - Specifies that the specified password is an encrypted password.

- **password**
  - Configures an authentication user-password for the NAI-constructed user.

  - `user_password` must be an alpha and/or numeric string of 0 through 63 characters in length.

- **use-shared-secret-password**
  - Specifies using RADIUS shared secret as the password.
  - Default: No Password

**Usage**

This command is used to configure passwords for user sessions that utilize a constructed NAI assigned via a PDSN service or a user name assigned via the APN configuration. For simple IP sessions facilitated by PDSN services in which the `authentication allow-noauth` and `aaa constructed-nai` commands are configured, this command provides a password used for the duration of the session.

For PDP contexts using an APN in which the outbound user name is configured with no password, this command is used to provide the password. Additionally, this command is also used to provide a password for situations in which an outbound username and password are configured and the `authentication imsi-auth` command has been specified.

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

If a password is configured with this keyword, then the specified password is used. Otherwise, an empty user-password attribute is sent.

Note that this configuration works in a different way for GGSN services. If a password is configured with this keyword for GGSN service, the specified password is used. Otherwise, if an outbound password is
configured, that password is used. If no outbound password is configured, the RADIUS server secret is used as the user-password string to compute the user-password RADIUS attribute.
The NAI-construction consists of the subscriber’s MSID, a separator character, and a domain. The domain that is used is either the domain name supplied as part of the subscriber’s user name or a domain alias.

**Important:** The domain alias can be set with the `nai-construction domain` command in the PDSN Service Configuration mode, or the `aaa default-domain subscriber` command in the Global Configuration mode for other core network services.

The domain alias is determined according to the following rules:
- If the domain alias is set by `nai-construction domain`, that value is always used and the `aaa default-domain subscriber` value is disregarded, if set. The NAI is of the form `<msid><symbol><nai-construction domain>`.
- If the domain alias is not set by `nai-construction domain` and the domain alias is set by `aaa default-domain subscriber`, the `aaa default-domain subscriber` value is used. The NAI is of the form `<msid><symbol><aaa default-domain subscriber>`.
- If the domain alias is not set by `nai-construction domain` or `aaa default-domain subscriber`, the domain name alias is the name of the source context for the PDSN service. The NAI is of the form `<msid><symbol><source context of PDSN Service>`.

The special separator character can be one of the following six: @, -, %, \, /.
The subscriber’s MSID is constructed in one of the formats displayed in the following figure.

<table>
<thead>
<tr>
<th>Mobile Country Code (3 digits)</th>
<th>Mobile Network Code (2 or 3 digits)</th>
<th>Mobile Subscriber Identification Number (10 digits max)</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Mobile Station Identity (IMSI)</td>
<td>Area Code (3 digits)</td>
<td>Office Code (3 digits)</td>
</tr>
<tr>
<td>Mobile Identification Number (MIN)</td>
<td>Mobile Country Code (3 digits)</td>
<td>Mobile Network Code (1 digit)</td>
</tr>
<tr>
<td>International Roaming MIN (IRM)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example

`aaa constructed-nai authentication`
`aaa constructed-nai authentication use-shared-secret-password`
aaa constructed-nai
aaa filter-id rulebase mapping

This command configures the system to use value of the Filter-Id AVP as the ACS rulebase name.

Product
ACS

Privilege
Security Administrator, Administrator

Syntax

[ no | default ] aaa filter-id rulebase mapping

no
Disables the mapping of Filter-Id AVP and ACS rulebase name.

default
Configures the default setting.
Default: Disabled; same as no aaa filter-id rulebase mapping

Usage
Use this command to enable the mapping of Filter-Id attribute’s value returned during RADIUS authentication as the ACS rulebase name.
This feature provides the flexibility for operator to transact between multi-charging-service support for postpaid and prepaid subscribers through Access Control Lists (ACLs) entered in AAA profiles in RADIUS server to single-charging-service system based on rulebase configuration for postpaid and prepaid subscribers.
This feature internally maps the received ACL in to rulebase name and configures subscriber for postpaid or prepaid services accordingly.
When this feature is enabled and ACS rulebase attribute is not received from RADIUS or not configured in local default subscriber template system copies the filter-id attribute value to ACS rulebase attribute.
This copying happens only if the filter-id is configured and received from RADIUS server and ACS rulebase is not configured in ACS or not received from RADIUS.

Example
Following command enables the mapping value of the Filter-Id attribute to ACS rulebase name:

aaa filter-id rulebase mapping
aaa group

This command enables creating/configuring/deleting AAA server groups in the context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

aaa group group_name [ -noconfirm ]
no aaa group group_name

group_name
Specifies the AAA group’s name.
If the specified AAA group does not exist, it is created, and the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.
If the specified AAA group already exists, the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.
group_name must be a string of 1 through 63 characters in length.

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

Usage
Use this command to create/configure/delete AAA server groups within the context. Also, refer to the AAA Server Group Configuration Mode chapter.

Example
The following command creates a AAA group named test321, and enters the AAA Group Configuration Mode:

aaa group test321
aaa nai-policy

This command sets policies on how NAIs (Network Access Identifiers) are handled during the authentication process.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] aaa nai-policy reformat-alg-hex-0-9
```

- **default**
  Sets the NAI policy back to its default setting which is to remap hexadecimal digits in NAIs and accept calls with embedded 0x00 hexadecimal digits.

- **no**
  Disable remapping of hexadecimal digits in the NAI and reject calls that have a 0x00 hexadecimal digit embedded in the NAI

- **reformat-alg-hex-0-9**
  Default: Enabled
  This keyword controls remapping of NAIs that consist only of hex digits 0x00 through 0x09 or if a 0x00 hexadecimal digit is embedded in the NAI.
  By default, the system remaps NAIs that consist solely of characters 0x00 through 0x09 to their ASCII equivalent. For example; 0x00 0x01 0x2 0x03 will get remapped to 123.
  Also by default the system accepts an NAI containing one or more 0x00 characters within the NAI ignoring all characters after the first 0x00.
  When this keyword is disabled NAIs are processed as follows:
  - Remapping of hexadecimal digits 0x00 through 0x09 within the user-provided NAI is disabled.
  - When the NAI has an embedded 0x00 character anywhere within it (including if there is an extra 0x00 character at the end) the call is rejected.

**Usage**
Use this command to disable or re-enable remapping of hexadecimal digits in the NAI.

**Example**
The following command disables the remapping of hexadecimal digits in the NAI:

```
no aaa nai-policy reformat-alg-hex-0-9
```
**access-list undefined**

Configures the behavior of access control for the current context when an undefined access control list is specified.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
access-list undefined { deny-all | permit-all }
```

```
no access-list undefined
```

- **no**
  - Disables handling undefined access lists.

- **deny-all | permit-all**
  - Specifies the handling of packets when an undefined access control list is specified.
    - **deny-all**: Specifies all packets will be dropped.
    - **permit-all**: Specifies all packets will be forwarded.

**Usage**
Use this command to specify the default behavior when an access control list specified does not exist. When the security policies require strict access control the **deny-all** handling should be configured.

**Example**
The following command sets the packet handling to ignore (drop) all packets when an undefined ACL is specified.

```
access-list undefined deny-all
```
**administrator**

This command configures a user with security administrator privileges in the current context.

**Product**

All

**Privilege**

Security Administrator

**Syntax**

```
administrator user_name [ encrypted ] password password | [ ecs ] [ expiry-date date_time ] [ ftp ] [ li-administration ] [ nocli ] [ noecs ] [ timeout-absolute timeout_absolute ] [ timeout-min-absolute timeout_min_absolute ] [ timeout-idle timeout_idle ] [ timeout-min-idle timeout_min_idle ]

no administrator user_name
```

- `no` Removes security administrator privileges for the specified user name.

- `user_name` Specifies the user name for which security administrator privileges must be enabled in the current context. `user_name` must be an alpha and/or numeric string of 1 through 32 characters in length.

- `[ encrypted ] password password` Specifies password for the user name. Optionally, the `encrypted` keyword can be used to specify the password uses encryption. Without encryption, `password` must be an alpha and/or numeric string of 1 through 63 characters in length. With encryption, `password` can be an alpha and/or numeric string of 1 through 127 characters in length. The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

- `ecs` Permits the user to use ACS-specific configuration commands. Default: Permitted.

- `expiry-date date_time` Specifies the date and time that this login account expires. Enter the date and time in the YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss format. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

- `ftp` Permits the user to use FTP and SFTP.
Default: Not permitted.

**li-administration**
Permits the user to execute Lawful Intercept commands.

---

**Important:** Users who have Lawful Intercept privileges are only given those privileges when connected to the system through a Secure Shell (SSH). If this user connects through a Telnet session or through the console port, Lawful Intercept privileges are not enabled.

---

**nocli**
Default: Permitted. Prevents the user from using the command line interface.

**noecs**
Prevents the user from accessing ACS-specific commands.

**timeout-absolute** `timeout_absolute`
Specifies the maximum time, in seconds, the security administrator may have a session active before the session is forcibly terminated. `timeout_absolute` must be an integer from 0 through 30000000. The value 0 disables this timeout configuration.
Default: 0

**timeout-min-absolute** `timeout_min_absolute`
Specifies the maximum time, in minutes, the security administrator may have a session active before the session is forcibly terminated. `timeout_min_absolute` must be an integer from 0 through 525600 (365 days). The value 0 disables this timeout configuration.
Default: 0

**timeout-idle** `timeout_idle`
Specifies the maximum time, in seconds, the security administrator may have a session active before the session is terminated. `timeout_idle` must be an integer from 0 through 30000000.
The value 0 disables the idle timeout configuration.
Default: 0

**timeout-min-idle** `timeout_min_idle`
Specifies the maximum time, in minutes, the security administrator may have a session active before the session is terminated. `timeout_min_idle` must be an integer from 0 through 525600 (365 days). The value 0 disables the idle timeout configuration.
Default: 0

---

**Usage**
Use this command to create new security administrators or modify existing user’s settings. Security Administrator users have read-write privileges and full access to all contexts and command modes. Refer to the Command Line Interface Overview chapter for more information.
**Important:** A maximum of 128 administrative users and/or subscribers may be locally configured per context.

---

**Example**
The following command creates a security administrator named `user1` with access to ACS configuration commands:

```
administrator user1 password secretPassword
```

The following removes the security administrator account named `user1`:

```
no administrator user1
```
Context Configuration Mode Commands

apn

Creates/deletes Access Point Name (APN) templates and enters the APN configuration mode within the current context.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Syntax

```
apn apn_name[ -noconfirm ]
no apn apn_name[ -noconfirm ]
```

**no**
Deletes a previously configured APN template.

**apn_name**
Specifies a name for the APN template.

*apn_name* can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-).

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

⚠️ **WARNING:** If this keyword option is used with *no apn apn_name* command the APN named *apn_name* will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage
This command creates an APN within the system and causes the CLI to enter the APN configuration mode. The APN is a logical name for a packet data network and/or a service to which the system supports access. When a create PDP context request is received by the system, it examines the APN information element within the packet. The system determines if an APN with the identical name is configured. If so, the system uses the configuration parameters associated with that APN as a template for processing the request. If the names do not match, the request is rejected with a cause code of 219 (DBH, Missing or unknown APN). APN templates should be created/configured within destination contexts on the system. Up to 1000 APNs can be configured.

Example
The following command creates an APN template called isp1:

```
apn isp1
```
asn-qos-descriptor

Creates/deletes/manages the Quality of Service (QoS) descriptor table identifier for Access Service Node Gateway (ASN-GW) service and enters the ASN QoS Descriptor Table Identifier Configuration mode within the source context.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

asn-qos-descriptor id <qos_table_id> [default] dscp [be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af 42 | af 43 | ef][-noconfirm ]

no asn-qos-descriptor qwos_table_id [default] dscp [be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af 42 | af 43 | ef][-noconfirm ]

no
Deletes a previously configured ASN QoS descriptor table identifier.

qos_table_id
Specifies an unique identifier for ASN QoS descriptor table to create/configure. qos_table_id must be an integer between 1 to 65535.

[default] dscp
Specifies DSCP marking for this QoS descriptor.

[be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af 42 | af 43 | ef]
The DSCP marking for this QoS descriptor. Default value is be (best effort).

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

⚠️ WARNING: If this keyword option is used with no asn-Qos-descriptor id <qos_table_id> command the ASN QoS descriptor table with identifier <qos_table_id> will be deleted with all active/inactive configurations without prompting any warning or confirmation.

Usage
Use this command to configure a QoS description table to manage QoS functionality for an ASN-GW service subscriber. This command creates and allows the configuration of QoS tables with in a context. This command is also used to remove previously configured ASN-GW services QoS descriptor table. A maximum of 16 QoS Descriptor Tables can be configured per system. Refer to the ASN QoS Descriptor Configuration Mode chapter of this reference for additional information.

Example
The following command creates a QoS descriptor table with identifier 1234 for the ASN-GW service subscribers:
asn-qos-descriptor id 1234
asn-service-profile

Creates/deletes/manages the Service Profiles Identifier for Access Service Node Gateway (ASN-GW) service subscribers and enters the ASN Service Profile Configuration mode within the current context.

Product
ASN-GW

Privilege
Administrator

Syntax

```
asn-service-profile idasn_profile_id direction { bi-directional | downlink | uplink } [ -noconfirm ]

no asn-service-profile idasn_profile_id[ -noconfirm ]
```

**no**
Deletes a previously configured ASN service profile identifier.

**qos_table_id**
Specifies an unique identifier for ASN QoS descriptor table to create/configure.
`qos_table_id` must be an integer between 1 to 65535.

**direction { bi-directional | downlink | uplink }**
Specifies the direction of data traffic to apply this service profile.

- **bi-directional**: This keyword enables this service profile in both direction of uplink and downlink.
- **downlink**: This keyword enables this service profile in downlink direction, towards the subscriber.
- **uplink**: This keyword enables this service profile in uplink direction, towards the system.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**WARNING**: If this keyword option is used with `no asn-service-profile idasn_profile_id` command the ASN service profile with identifier `asn_profile_id` will be deleted with all active/inactive configurations without prompting any warning or confirmation.

**Usage**

Use this command to configure a service profile to apply the ASN-GW service subscribers. This command creates and allows the configuration of service profiles with in a context. This command is also used to remove previously configured ASN-GW services profiles.

A maximum of 32 ASN Service Profiles can be configured per context.

Refer to the ASN Service Profile Configuration Mode chapter of this reference for additional information.

**Example**

---

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01

927
The following command creates an ASN Service Profile with identifier 1234 for the ASN-GW service subscribers:

```
asn-service-profile id 1234 direction uplink
```
asngw-service

Creates/deletes/manages an Access Service Node Gateway (ASN-GW) service and enters the ASN Gateway service configuration mode within the current context.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

\texttt{asngw-service} \texttt{asngw\_name[-noconfirm ]}
\texttt{no asngw-service} \texttt{asngw\_name[-noconfirm ]}

\texttt{no}
Deletes a previously configured ASN-GW service.

\texttt{asngw\_name}
Specifies the name of the ASN-GW service to create/configure.\texttt{asngw\_name} must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

\texttt{-noconfirm}
Indicates that the command is to execute without any additional prompt and confirmation from the user.

\textbf{WARNING:} If this keyword option is used with \texttt{no asngw-service asngw\_name} command the ASN-GW service named \texttt{asngw\_name} will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage
Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as an ASN Gateway in a WiMAX network. This command is also used to remove previously configured ASN-GW services. A maximum of 256 services (regardless of type) can be configured per system.

\textbf{Caution:} Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the ASN Gateway Service Configuration Mode chapter of this reference for additional information.

Example
The following command creates an ASN-GW service name \texttt{asn\_gw1}:
asngw-service

asngw-service  asn-gwl
asnpc-service

This command Creates/deletes/manages an ASN Paging Controller service to manage the ASN paging controller service and enters the ASN Paging Controller Configuration mode within the current context.

Product
ASN GW

Privilege
Security Administrator, Administrator

Syntax

[no] asnpc-service asn_pc_svc_name [-noconfirm]

- no
  Deletes a previously configured ASN paging controller service.

- asn_pc_svc_name
  Specifies the name of the ASN Paging Controller Service to create and enable.
  asn_pc_svc_name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- -noconfirm
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

⚠️ WARNING: If this keyword option is used with no asnpc-service asn_pc_svc_name command the ASN Paging Controller service named asn_pc_svc_name will be deleted and disabled with all active/inactive paging groups and paging agents configured in a context for ASN paging controller service without prompting any warning or confirmation.

Usage

Use this command to create and enable the ASN paging controller services in the system to provide functionality of an ASN Paging Controller service within a context. Additionally this command provides the access to the ASN Paging Controller Service Configuration mode and also used to remove previously configured ASN Paging Controller services.
A maximum of 256 services (regardless of type) can be configured per system.

⚠️ Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the ASN Paging Controller Service Configuration Mode chapter of this reference for additional information.

Example
The following command creates an ASN paging controller service name `asnpc_1`:

```
asnpc-service asnpc_1
```
**bsmc-profile**

Creates/deletes Broadcast Multicast Service Center (BM-SC) profiles and enters the BMSC Profile configuration mode within the current context.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bsmc-profile name bmsc_profile_name [-noconfirm ]
```

- no bmsc-profile name bmsc_profile_name [-noconfirm ]

**no**
Deletes a previously configured BM-SC profile.

**bsmc_profile_name**
Specifies a name for the BM-SC profile.
`bsmc_profile_name` can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-).

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

⚠️ **WARNING:** If this keyword option is used with `no bmsc-profile name bmsc_profile_name` command the BM-SC profile named `bmsc_profile_name` will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

**Usage**
This command creates a BM-SC profile within the context and take the user to enter the BMSC profile configuration mode.
The BM-SC profile is a logical name for a Broadcast Multicast Service Center in Multimedia Broadcast and Multicast service.
BM-SC profile should be created/configured within contexts on the system. Up to 4 BM-SC profiles can be configured.

**Example**
The following command creates a BM-SC Profile called `mbms_sc_1`:

```
bsmc-profile name mbms_sc_1
```
busouit ip pool

This command makes addresses from an IP pool in the current context unavailable once they are free.

Product
PDSN, HA, GGSN, NAT

Privilege
Security Administrator, Administrator

Syntax

busouit ip pool { all | all-dynamic | all-static | name pool_name } [ address-range start_address end_address | lower-percentage percent | upper-percentage percent ]

no busouit ip pool { all | all-dynamic | all-static | name pool_name } [ address-range start_address end_address | lower-percentage percent | upper-percentage percent ]

no
Disable the busouit command specified.

all
This command applies to all IP pools in the current context.

all-dynamic
This command applies to all dynamic IP-pools in the current context.

all-static
This command applies to all static IP pools in the current context.

name pool_name
This is the name of an IP pool or IP pool group in the current context to which this command is applied.
pool_name must be the name of an existing IP pool or IP pool group in the current context.

address-range start_address end_address
Busouit all addresses from start_address through end_address. start_address: The beginning IP address of the range of addresses to busouit. This IP address must exist in the pool specified and must be entered in IP v4 dotted decimal notation.
end_address: The ending IP address of the range of addresses to busouit. This IP address must exist in the pool specified and must be entered in IP v4 dotted decimal notation.

lower-percentage percent
Busouit the percentage of IP addresses specified, beginning at the lowest numbered IP address. This is a percentage of all of the IP addresses in the specified IP pool. percent must be an integer from 0 through 100.
**upper-percentage percent**

Busyout the percentage of IP addresses specified, beginning at the highest numbered IP address. This is a percentage of all of the IP addresses in the specified IP pool. `percent` must be an integer from 0 through 100.

**Usage**

Use this command to busyout IP addresses when resizing an IP pool.
Up to 32 instances of this command can be executed per context.
A single instance of this command can busy-out multiple IP address pools in the context through the use of the `all.all-static` or `all-dynamic` keywords.

**Example**

Assume an IP pool named Pool10 with addresses from 192.168.100.1 through 192.168.100.254. To busy out the addresses from 192.168.100.50 through 192.169.100.100, enter the following command:

```
busyout ip pool name Pool10 address-range 92.168.100.50 192.169.100.100
```

To restore the IP addresses from the previous example and make them accessible again, enter the following command:

```
no busyout ip pool name Pool10 address-range 92.168.100.50 192.169.100.100
```
**class-map**

This command deletes/creates and enters the Class-Map configuration mode within the current destination context to configure the match rules for packet classification to flow-based traffic policing for a subscriber session flow.

**Product**
PDSN, HA, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] class-map name class_name [ match-all | match-any ]
```

- **no**
  Deletes configured Class-Map within the context.

- **class_name**
  Specifies the name of Class-Map rule and can consist of from 1 to 15 alpha and/or numeric characters in length and is case sensitive.

- **match-all**
  Default: Enabled.
  Enables AND logic for all matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match all classification rules in specific Class-Map to consider the specified Class-Map as a match.

- **match-any**
  Default: Disabled.
  Enables OR logic for matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match any of the classification rule in specific Class-Map to consider the specified Class-Map as a match.

**Usage**

Use this command to enter in Class-Map configuration mode to set classification parameters or filters in traffic policy for a subscriber session flow.

**Important:** In this mode classification rules added sequentially with match command to form a Class-Map. To change and/or delete or re-add a particular rule entire Class-Map is required to delete.

**Example**
Following command configures classification map class_map1 with option to match any condition in match rule.

```
class-map name class_map1 match-any
```
closedrp-rp handoff

This command enables session handoff between Closed-RP and RP connections. Default: Disabled

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

closedrp-rp handoff

[ default | no ] closedrp-rp handoff

default
Resets the command to its default setting of disabled.

no
Disables Closed-RP to RP session handoff.

Usage
Use this command to enable a PDSN service to handoff sessions between Closed-RP and RP connections.

Example
To enable Closed-RP to RP handoffs, use the following command:

closedrp-rp handoff

To disable Closed-RP to RP handoffs, use the following command:

no closedrp-rp handoff
config-administrator

Configures a context-level administrator account within the current context.

Product
All

Privilege
Security Administrator

Syntax

config-administrator user_name [ encrypted ] password pwd [ ecs ] [ expiry-date date_time ] [ ftp ] [ li-administration ] [ nocli ] [ noecs ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [ timeout-idle idle_seconds ] [ timeout-min-idle idle_minutes ]

no config-administrator user_name

no
Removes a previously configured context-level administrator account.

user_name
Specifies the name for the account. user_name must be from 1 to 32 alpha and/or numeric characters.

[ encrypted ] password pwd
Specifies the password to use for the user which is being given context-level administrator privileges within the current context. The encrypted keyword indicates the password specified uses encryption. The password specified as pwd must be from 1 to 63 alpha and/or numeric characters without encryption and must be from 1 to 127 alpha and/or numeric characters when encryption has been indicated. The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

ecs
Default: ACS-specific configuration commands allowed. Permits the specific user to access ACS-specific configuration commands.

expiry-date date_time
The date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

ftp
Default: FTP and SFTP are not allowed. Indicates the user gains FTP and SFTP access with the administrator privileges.
## li-administration
Permits this user to execute Lawful Intercept commands.

### Important:
Users who have Lawful Intercept privileges are only given those privileges when connected to the system through a Secure Shell (SSH). If this user connects through a Telnet session or through the console port, Lawful Intercept privileges are not enabled.

### nocli
Default: CLI access allowed.
Indicates the user is not allowed to access the command line interface.

### noecs
Prevents the specific user to access ACS-specific configuration commands.

### timeout-absolute abs_seconds
Default: 0
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of time, in seconds, the administrator may have a session active before the session is forcibly terminated. abs_seconds must be a value in the range from 0 through 300000000.
The special value 0 disables the absolute timeout.

### timeout-min-absolute abs_minutes
Default: 0
Specifies the maximum amount of time, in minutes, the context-level administrator may have a session active before the session is forcibly terminated. abs_minutes must be a value in the range from 0 through 525600 (365 days).
The special value 0 disables the absolute timeout.

### timeout-idle idle_seconds
Default: 0
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of idle time, in seconds, the context-level administrator may have a session active before the session is terminated. idle_seconds must be a value in the range from 0 through 300000000.
The special value 0 disables the idle timeout.

### timeout-min-idle idle_minutes
Default: 0
Specifies the maximum amount of idle time, in minutes, the context-level administrator may have a session active before the session is terminated. idle_minutes must be a value in the range from 0 through 525600 (365 days).
The special value 0 disables the idle timeout.
Create new context-level administrators or modify existing administrator’s options, in particular, the timeout values. Administrator users have read-write privileges and full access to all contexts and command modes (except for a few security functions). Refer to the Command Line Interface Overview chapter of this guide for more information.

**Important:** A maximum of 128 administrative users and/or subscribers may be locally configured per context.

**Example**
The following configures a context-level administration named user1 with ACS parameter control:

```
config-administrator user1 password secretPassword ecs
```

The following command removes a context-level administrator named user1:

```
no config-administrator user1
```
content-filtering

This command enables creating/configuring/deleting Content Filtering Server Groups (CFSG).

Product
CF

Privilege
Security Administrator, Administrator

Syntax

```
content-filtering server-group cf_server_group_name [ -noconfirm ]
no content-filtering server-group cf_server_group_name
```

**no**
Removes the specified CFSG previously configured in this context.

**cf_server_group**
Specifies the CFSG name.
`cf_server_group_name` must be an alpha and/or numeric string of 1 through 63 characters in length.

**-noconfirm**
Creates the specified CFSG without prompting for confirmation.

Usage
Use this command to create/configure/delete a CFSG.

Example
The following command creates a CFSG named `CF_Server1`:
```
content-filtering server-group CF_Server1
```
credit-control-service

This command enables creating/configuring/deleting credit-control services.

Product
All

Privilege
Security Administrator, Administrator

Syntax

credit-control-service service_name [ -noconfirm ]

no credit-control-service service_name

no
Deletes the specified credit-control service.

service_name
Specifies the credit-control service’s name.
service_name must be an alpha and/or numeric string of 1 through 63 characters in length.
If the named credit-control service does not exist, it is created, and the CLI mode changes to the Credit Control Service Configuration mode wherein the service can be configured.
If the named credit-control service already exists, the CLI mode changes to the Credit Control Service Configuration mode wherein the service can be configured.

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

Usage
Use this command to create/configure/delete credit-control services.

Example
The following command creates a credit-control service named test159, and enters the Credit control Service Configuration mode:

credit-control-service test159
crypto group

Creates a crypto group and enters the crypto configuration mode allowing the configuration of crypto group parameters.

Product

PDSN, PDIF, HA, GGSN, SCM

Privilege

Administrator, Config-Administrator

Syntax

crypto group group_name

no crypto group group_name

Example

The following command configures a crypto group called group1:

crypto group group1
Crypto Infosec Transform-Set

Crypto Infosec Transform-set

Configures transform-sets on the system and enters the Crypto Trans Configuration Mode.

Product
PDSN, PDIF, HA, GGSN, SCM

Privilege
Security Administrator, Administrator

Syntax

crypto ipsec transform-set transform_name

Ah { hmac { md5-96 | none | sha1-96 } } esp { hmac { md5-96 | sha1-96 } } cipher { des-cbc | 3des-cbc | aes-cbc } }

no crypto ipsec transform-set transform_name

no
Removes a previously configured transform set

transform_name
Configures the name by which the transform set will be recognized by the system.
transform_name must be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Ah hmac
Configures the Authentication Header (AH) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

• md5-96: Message Digest 5 truncated to 96 bits
• none: Disables the use of the AH protocol for the transform set.
• sha1-96: Secure Hash Algorithm-1 truncated to 96 bits

Esp hmac
Configures the Encapsulating Security Payload (ESP) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

• md5-96: Message Digest 5 truncated to 96 bits
• none: Disables the use of the AH protocol for the transform set.
• sha1-96: Secure Hash Algorithm-1 truncated to 96 bits

cipher
If ESP is enabled, this option must be used to set the encapsulation cipher protocol to one of the following:

• 3des-cbc: Triple Data Encryption Standard (3DES) in chain block (CBC) mode
• aes-cbc: Advanced Encryption Standard (AES) in CBC mode
• des-cbc: DES in CBC mode
crypto ipsec transform-set

Usage
Use this command to create a transform set on the system.
Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.
Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

Important: The ah and subsequent keywords are required when the transform set is initially configured.

Example
Create a transform set that has the name tset1, no authentication header, an encapsulating security protocol header hash message authentication code of md5, and a bulk payload encryption algorithm of des-cbc with the following command:

crypto ipsec transform-set tset1 ah hmac none esp hmac md5 cipher des-cbc
crypto map

Configures the name of the policy and enters either the specified Crypto Map Configuration Mode.

Product
PDSN, HA, GGSN, SCM, P-GW, PDIF

Privilege
Security Administrator, Administrator

Syntax

```
crypto map name [ ikev2-ipv6 | ipsec-dynamic | ipsec-ikev1 | ipsec-manual ] no
```

no
Removes a previously configured crypto map.

```
name
```

The name by which the crypto map will be recognized by the system. `name` must be a string of from 1 through 127 alpha and/or numeric characters and is case sensitive.

```
ikev2-ipv6
```

Creates an IKEv2-IPv6 crypto map and enters the Crypto Map IKEv2-IPv6 configuration mode.

```
ipsec-dynamic
```

Creates a dynamic crypto map and/or enters the Crypto Map Dynamic Configuration Mode.

```
ipsec-ikev1
```

Creates an IKEv1 crypto map and/or enters the Crypto Map IKEv1 Configuration Mode.

```
ipsec-manual
```

Creates a manual crypto map and/or enters the Crypto Map Manual Configuration Mode.

Usage

Crypto Maps define the policies that determine how IPSec is implemented for subscriber data packets. There are several types of crypto maps supported by the system. They are:

- **Manual crypto maps**: These are static tunnels that use pre-configured information (including security keys) for establishment. Because they rely on statically configured information, once created, the tunnels never expire; they exist until their configuration is deleted.

**Important**: Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.
IKEv1 crypto maps: These tunnels are similar to manual crypto maps in that they require some statically configured information such as the IP address of a peer security gateway and that they are applied to specific system interfaces. However, IKEv1 crypto maps offer greater security because they rely on dynamically generated security associations through the use of the Internet Key Exchange (IKE) protocol.

IKEv2-IPv6 crypto maps: Used to protect X3 data between a P-GW and a Lawful Intercept server.

Dynamic crypto maps: These tunnels are used for protecting L2TP-encapsulated data between the system and an LNS/security gateway or Mobile IP data between an FA service configured on one system and an HA service configured on another.

Important: The crypto map type (dynamic, IKEv1, IKEv2-IPv6, or manual) is specified when the map is first created using this command.

Example
Create a dynamic crypto map named map1 and enter the Crypto Map Dynamic configuration mode by entering the following command:

```
crypto map map1 ipsec-dynamic
```
crypto node

Creates a crypto node.

Product
SCM

Privilege
Administrator, Config-Administrator

Syntax

crypto node node_name map name

no crypto node node_name

node_name

The name of the crypto node and can consist of from 1 to 127 alpha and/or numeric characters in length and is case sensitive.

map name

Assigns a previously configured crypto map policy to this crypto node. name must be a string of from 1 through 127 alpha and/or numeric characters and is case sensitive.

no

Deletes a previously configured crypto node.

Usage

Use this command to configure a crypto node and assign policies (crypto maps) to the node.

Example

The following command configures a crypto node called node1 and assigns a policy named map1 to it:

crypto node node1 map map1
**crypto template**

Creates a new, or specifies an existing, crypto template and enters the Crypto Template Configuration Mode.

**Product**

PDIF, SCM

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
crypto template name { ikev2-pdif | ipsec-3gpp-cscf }
no crypto template name
```

`name { ikev2-pdif | ipsec-3gpp-cscf }`

Specifies the name of a new or existing crypto template. `name` must be from 1 to 127 alpha and/or numeric characters.

`ikev2-pdif`: Configure the Crypto Template to be used for configuring PDIF functionality.

**Important:** This keyword cannot be used with IPSec for the SCM.

`ipsec-3gpp-cscf`: Configure the Crypto Template to be used for configuring P-CSCF IPSec functionality.

**Important:** This keyword can only be used with IPSec for the SCM.

**Usage**

Use this command to create a new or enter an existing PDIF or P-CSCF crypto template.

**Important:** The CSCF crypto template should be configured in the same context in which the P-CSCF is configured.

Entering this command results in one of the following prompts:

```
[context_name]hostname(cfg-crypto-tmpl-ikev2-tunnel)#
[context_name]hostname(cfg-crypto-tmpl-ims-cscf-tunnel)#
```

Crypto Template Configuration Mode commands are defined in the *Crypto Template Configuration Mode Commands* and *CSCF Crypto Template Configuration Mode Commands* chapters.

**Example**

The following command configures a PDIF crypto template called `crypto1` and enters the Crypto Template Configuration Mode:

```plaintext
crypto template crypto1 ikev2-pdif
```
The following command configures a P-CSCF crypto template called `crypto2` and enters the CSCF Crypto Template Configuration Mode:

```
crypto template crypto2 ipsec-3gpp-cscf
```
The commands in this section are used for configuring parameters associated with the CSCF service.
cscf access-profile

Creates a new or enters an existing access profile used to set signaling compression for various network access types.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

cscf access-profile { default | name profile_name [ -noconfirm ] }

no cscf access-profile name profile_name

default
Specifies that the system is to enter the Access Profile Configuration Mode for the default access profile.

name profile_name
Specifies a name for the access profile.
profile_name must be from 1 to 79 alpha and/or numeric characters.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Use this command to create an access profile for the CSCF service and cause the system to enter the Access Profile Configuration Mode where parameters are configured for the profile.
Entering this command results in the following prompt:
[context_name]hostname(config-cscf-access-profile)#
Access Profile Configuration Mode commands are defined in the **CSCF Access Profile Configuration Mode Commands** chapter.

Example
The following command creates a CSCF Access Profile named profile2 and enters the Access Profile Configuration Mode:

cscf access-profile name profile2
cscf acl

Creates an access control list (ACL) and enters the ACL Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

cscf acl { default | name list_name [ -noconfirm ] }

no cscf acl name list_name

default
Specifies that the system is to enter the ACL Configuration Mode for the default ACL.

name list_name
Specifies a name for the ACL.
list_name must be from 1 to 47 alpha and/or numeric characters in length.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Use this command to create an access control list for the CSCF service and cause the system to enter the ACL Configuration Mode where parameters are configured for the new list. Entering this command results in the following prompt:
[context_name]hostname(config-cscf-acl)#
ACL Configuration Mode commands are defined in the CSCF ACL Configuration Mode Commands chapter. Use this command when configuring the following SCM components: P-CSCF, S-CSCF, and SIP Proxy.

Example
The following command creates a CSCF access control list named acl1 and enters the ACL Configuration Mode:

cscf acl name acl1
cscf ifc-filter-criteria

Creates Initial Filter Criteria (iFC) filter criteria for shared iFC functionality.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

cscf ifc-filter-criteria name fc_name priority pri profile-part-indicator { registered | unregistered } app-server uri scheme { sip | sips } as as-default-handling { session-continue | session-terminate } [ -noconfirm ] | [ service-info info ]{ trigger-point tp_name } [ -noconfirm ] | [ trigger-point tp_name ] [ -noconfirm ]

no cscf ifc-filter-criteria name fc_name

name fc_name
Specifies a name for the iFC filter criteria.
f_c_name must be from 1 to 39 alpha and/or numeric characters in length.

priority pri
Specifies the priority of the filter criteria, which is used to select a particular filter criteria from multiple ones present under an ISC template.
pri must be an integer from 0 through 1024.

profile-part-indicator { registered | unregistered }
Indicates whether the iFC is a part of the registered (registered) or unregistered (unregistered) user profile.

app-server uri scheme { sip | sips }
Determines the associated application server’s uri scheme.
sip: sip uri
sips: sips uri

as
Specifies an address for the associated application server.
as must be from 1 to 127 alpha and/or numeric characters in length.

as-default-handling { session-continue | session-terminate }
Determines whether the dialog should be released (session-terminate) or not (session-continue) if the application server could not be reached or on application server error return.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.
---

**service-info** *info*

Specifies optional service information to be sent to the application server. *info* must be from 1 to 63 alpha and/or numeric characters in length.

**trigger-point** *tp_name*

Assigns an iFC trigger point to the filter criteria. *tp_name* must be from 1 to 39 alpha and/or numeric characters in length.

**no cscf ifc-filter-criteria name** *fc_name*

Removes the specified CSCF iFC filter criteria from the context.

---

**Usage**

Use this command to create a filter criteria name and associate an application server address to it. You may also define a trigger point name to be executed in order to select the application server. If no trigger point is specified, then the application server is selected unconditionally.

---

**Important:** Filter criteria is associated with an ISC template in the ISC Template Configuration Mode.

**Important:** Filter criteria can be assigned to more than one ISC template.

---

**Example**

The following command creates an iFC filter criteria named *ifcfcl*, which has a priority of 2 and is part of the registered user profile. *ifcfcl* is assigned to a sip application server named *appserver*. The dialog will not be released if the application server can not be reached. *ifcfcl* is also assigned a trigger point named *tp2*:

```
cscf ifc-filter-criteria name ifcfcl priority 2 profile-part-indicator registered app-server uri scheme sip appserver as-default-handling session-continue trigger-point tp2
```
cscf ifc-spt-condition

Creates an Initial Filter Criteria (iFC) Service Point Trigger (SPT) condition for shared iFC functionality.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

cscf ifc-spt-condition name cond_name { request-uri content uri_content | session-case { originating-registered | originating-unregistered | terminating-registered | terminating-unregistered } | session-description sdp [ content sdp_data ] | sip-header hdr [ content hdr_data ] | sip-method method } [ -noconfirm ] [ condition-negated ]

no cscf ifc-spt-condition name cond_name

name cond_name
Specifies a name for the iFC SPT condition.
cond_name must be from 1 to 39 alpha and/or numeric characters in length.

request-uri content uri_content
Specifies request uri content.
uri_content must be from 1 to 127 alpha and/or numeric characters in length.

Important: Wildcard Extended Regular Expressions (ERE) are supported for this value. For example, “sip.user[0-9]@[192.168.176.150”

session-case (originating-registered | originating-unregistered | terminating-registered | terminating-unregistered)
Determines the type of session:
• originating-registered: Session handling an originating end user.
• originating-unregistered: Session handling an unregistered originating end user.
• terminating-registered: Session handling a terminating registered end user.
• terminating-unregistered: Session handling a terminating unregistered end user.

session-description sdp [ content sdp_data ]
Specifies an SDP line type.
sdp must be from 1 to 15 alpha and/or numeric characters in length.
content specifies content on the SDP line.
sdp_data must be from 1 to 127 alpha and/or numeric characters in length.

sip-header hdr [ content hdr_data ]
Specifies a header type.
cscf ifc-spt-condition

hdr must be from 1 to 127 alpha and/or numeric characters in length.
content specifies content on the header.
hdr_data must be from 1 to 127 alpha and/or numeric characters in length.

sip-method method
Specifies a sip method.
method must be from 1 to 127 alpha and/or numeric characters in length.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

condition-negated
Negates the specified condition.

no cscf ifc-spt-condition name cond_name
Removes the specified CSCF iFC SPT condition from the context.

Usage
Use this command to create individual SPT conditions that are later associated with an SPT group in the iFC SPT Group Configuration Mode.

Important: An iFC SPT group may be associated with multiple SPT conditions.

Example
The following command creates an iFC SPT condition named cond2 which handles an originating end user:

cscf ifc-spt-condition name cond2 session-case originating-registered

The following command negates the condition created above:

cscf ifc-spt-condition name cond2 session-case originating-registered condition-negated
cscf ifc-spt-group

Creates an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group for shared iFC functionality.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

```
cscf ifc-spt-group name group_name [ -noconfirm ] | reg-type { de-registration | initial-registration | re-registration } [ -noconfirm ]

no cscf ifc-spt-group name group_name
```

- **name group_name**
  Specifies a name for the iFC SPT group.
  `group_name` must be from 1 to 39 alpha and/or numeric characters in length.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

- **reg-type { de-registration | initial-registration | re-registration }**
  Defines whether the SPT condition matches to REGISTER messages that are related to:
  - de-registration
  - initial-registration
  - re-registration

```
no cscf ifc-spt-group name group_name
```

Removes the specified CSCF iFC SPT group from the context.

Usage

Use this command to create an iFC SPT group name and bind different SPT conditions under it.

**Important:** An iFC SPT group may be associated with multiple SPT conditions.

The SPT group can also specify the registration type that defines whether the SPT condition matches to REGISTER messages that are related to initial registrations, re-registrations, or de-registrations.
Entering this command results in the following prompt:
```
[context_name]hostname(config-cscf-ifc-spt-group)#
```
iFC SPT Group Configuration Mode commands are defined in the **CSCF IFC SPT Group Configuration Mode Commands** chapter.
Example
The following command creates an iFC SPT group named *group2*:

```
cscf ifc-spt-group name group2
```
cscf ifc-trigger-point

Creates an Initial Filter Criteria (iFC) trigger point for shared iFC functionality.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

```
cscf ifc-trigger-point name tp_name condition-type { cnf | dnf } [ -noconfirm ]
```

```
no cscf ifc-trigger-point name tp_name
```

<table>
<thead>
<tr>
<th>name tp_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a name for the iFC trigger point. tp_name must be from 1 to 39 alpha and/or numeric characters in length.</td>
</tr>
</tbody>
</table>

| condition-type { cnf | dnf } |
|-----------------------------|
| Defines the condition type of the iFC trigger point: cnf: conjunctive normal form dnf: disjunctive normal form |

<table>
<thead>
<tr>
<th>-noconfirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates that the command is to execute without any additional prompt and confirmation from the user.</td>
</tr>
</tbody>
</table>

```
no cscf ifc-trigger-point name tp_name
```

Removes the specified CSCF iFC trigger point from the context.

Usage
Use this command to create a trigger point name and bind different SPT groups under it.

**Important:** An iFC SPT group can be assigned to more than one iFC trigger point.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-ifc-trigger-point)#
```

IFC Trigger Point Configuration Mode commands are defined in the **CSCF IFC Trigger Point Configuration Mode Commands** chapter.

Example
The following command creates an iFC trigger point named tp_2 with a cnf condition type:

```
cscf ifc-trigger-point name tp_2 condition-type cnf
```
csf ifc-trigger-point
**cscf isc-template**

Creates an IMS Service Control (ISC) template and enters the ISC Template Configuration Mode.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
[ no ] cscf isc-template name template_name
```

- **no**
  Removes the CSCF ISC template from the context.

- **name template_name**
  Specifies a name for the ISC template.
  *template_name* must be from 1 to 39 alpha and/or numeric characters in length.

**Usage**

Use this command to create an ISC template for the CSCF service and cause the system to enter the ISC Template Configuration Mode where parameters are configured for the new template.

Entering this command results in the following prompt:
```
[context_name]hostname(config-cscf-isc-tmpl)#
```

ISC Template Configuration Mode commands are defined in the *CSCF ISC Template Configuration Mode Commands* chapter.

Use this command when configuring the following SCM component: S-CSCF.

**Example**

The following command creates an ISC template named *template1* and enters the ISC Template Configuration Mode:

```
cscf isc-template name template1
```
cscf last-route-profile

Creates a last route profile, which will be specified on peer server configuration to select the Last Routing Option (LRO) number while forwarding an emergency call packet to a particular peering server, and enters the Last Route Profile Criteria Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

```plaintext
  cscf last-route-profile name profile_name criteria {county-name | round-robin} [-noconfirm ]
  no cscf last-route-profile name profile_name
```

**name** *profile_name*
Specifies the name of the last route profile.

*profile_name* must be from 1 to 79 alpha and/or numeric characters in length.

**criteria { county-name | round-robin }**

*county-name*: Profile specific to the county-name criteria.

Entering this command results in the following prompt:

```plaintext
[ccontext_name]hostname(config-county-name-lro-profile)#
```

Last Route Profile Criteria Configuration Mode commands are defined in the *CSCF Last Route Profile Criteria Configuration Mode Commands* chapter.

*round-robin*: Profile specific to the round-robin criteria.

Entering this command results in the following prompt:

```plaintext
[ccontext_name]hostname(config-round-robin-lro-profile)#
```

Last Route Profile Criteria Configuration Mode commands are defined in the *CSCF Last Route Profile Criteria Configuration Mode Commands* chapter.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**no cscf last-route-profile name profile**
Removes the specified CSCF last route profile from the context.

**Usage**

Use this command to create a last route profile and enter the Last Route Profile Criteria Configuration Mode.

**Important:** Last route profiles are associated with peer servers in the CSCF Peer Server Monitoring Configuration Mode.

Use this command when configuring the following SCM components: S-CSCF and SIP Proxy.
Example
The following command creates a last route profile named \texttt{lro1} and enters the CSCF Last Route Profile Criteria Configuration Mode to specify county name criteria:

\[ \text{cscf last-route-profile name lro1 criteria county-name} \]

The following command creates a last route profile named \texttt{lro2} and enters the CSCF Last Route Profile Criteria Configuration Mode to specify round robin criteria:

\[ \text{cscf last-route-profile name lro2 criteria round-robin} \]
**cscf peer-servers**

Creates a peer server group type for next-hop session routing and enters the Peer Server Configuration Mode.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrfc | pcscf | scscf | sip-as } [ -noconfirm ]
```

```
no cscf peer-servers server_name
```

- `server_name` Specifies the name of the peer server group.
  - `server_name` must be from 1 to 79 alpha and/or numeric characters in length.

- `type { bgcf | ibcf | icscf | mgcf | mrfc | pcscf | scscf | sip-as }`
  - Specifies the type of peer server group to configure:
    - `bgcf`: Border Gateway Control Function
    - `ibcf`: Interconnect Border Control Function
    - `icscf`: Interrogating-Call/Session Control Function
    - `mgcf`: Media Gateway Control Function
    - `mrfc`: Media Resource Function Controller
    - `pcscf`: Proxy-Call/Session Control Function
    - `scscf`: Serving-Call/Session Control Function
    - `sip-as`: Session Initiation Protocol-Application Server

- `-noconfirm`
  - Indicates that the command is to execute without any additional prompt and confirmation from the user.

```
no cscf peer-servers server_name
```

Removes the specified CSCF peer server group from the context.

**Usage**

Use this command to create a specific peer server group and enter the Peer Server Configuration Mode where connectivity parameters can be entered.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-peer-servers)#
```

Peer Servers Configuration Mode commands are defined in the *CSCF Peer Servers Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, and SIP Proxy.

Example
The following command creates an I-CSCF server group type called `icscf_group1` and enters the Peer Server Configuration Mode:

```
cscf peer.servers icscf_group1 type icscf
```
cscf policy

Creates a policy group for specific AoR profiles and enters the Policy Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

```
cscf policy { default | name policy_name [ -noconfirm ] }  
no cscf policy name policy_name
```

**default**

Specifies that the system is to enter the AoR Policy Rules Configuration Mode for the default policy. The default policy uses AoR policy rules.

Entering this command results in the following prompt:

```
[context_name]hostname(config-aor-policy)#
```

Default (AoR) Policy Configuration Mode commands are defined in the CSCF AoR Policy Rules Configuration Mode Commands chapter.

**name policy_name**

Specifies the name of the policy group.

_policy_name_ must be from 1 to 79 alpha and/or numeric characters in length.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-policy)#
```

Policy Configuration Mode commands are defined in the CSCF Policy Configuration Mode Commands chapter.

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**no cscf policy name policy_name**

Removes the specified CSCF policy group from the context.

**Usage**

Use this command to create a policy group and enter either the AoR Policy Rules Configuration Mode (**default**) or Policy Configuration Mode (**name policy_name**).

Use this command when configuring the following SCM components: P-CSCF, S-CSCF, and SIP Proxy.

**Example**

The following command creates a policy group named _group2_ and enters the CSCF Policy Configuration Mode:

```
cscf policy name group2
```
cscf routes

Creates a route group for specifying routing information and enters the Routes Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

cscf routes { default | name route_name [ -noconfirm ] }

no cscf routes name route_name

---

**default**
Specifies that the system is to enter the Routes Configuration Mode for the default route group.

**name route_name**
Specifies the name of the route group.
*route_name* must be from 1 to 79 alpha and/or numeric characters in length.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create a route group and enter the Routes Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-route)#
```

Routes Configuration Mode commands are defined in the *CSCF Routes Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

Example

The following command creates a route group named *route_group5* and enters the Route Group Configuration Mode:

```
cscf routes name route_group5
```
cscf service

 Creates a CSCF service or specifies an existing CSCF service and enters the CSCF service configuration mode for the current context.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```plaintext
cscf service service_name [ -noconfirm ]
no cscf service service_name
```

- `service_name`
  Specifies the name of the CSCF service. If `service_name` does not refer to an existing service, the new service is created if resources allow.
  `service_name` must be from 1 to 63 alpha and/or numeric characters.

- `-noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Enter the CSCF service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:
```
[context_name]@hostname(config-cscf-service)#
```
CSCF Service Configuration Mode commands are defined in the **CSCF Service Configuration Mode Commands** chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

**Example**
The following command enters the existing CSCF service configuration mode (or creates it if it doesn’t already exist) for the service named `cscf-service1`:
The following command will remove `cscf-service1` from the system:

```
no cscf service cscf-service1
```
cscf session-template

Creates a session template and/or enters the Session Template Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

```
cscf session-template { default | name template_name [ -noconfirm ] }
no cscf session-template name template_name
```

*default*
Specifies that the system is to enter the Session Template Configuration Mode for the default session template.

*name template_name*
Specifies a name for the template. `template_name` must be from 1 to 79 alpha and/or numeric characters in length.

*-noconfirm*
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create a new session template and enter the Session Template Configuration Mode or enter the mode for an existing template. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-session-template)#
```

Session Template Configuration Mode commands are defined in the *CSCF Session Template Configuration Mode Commands* chapter. Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

Example

The following command enters the Session Template Configuration Mode for a template named `sess_temp4`:

```
cscf session-template name sess_temp4
```
cscf translation

Creates/removes a translation list and/or enters the Translation Configuration Mode.

**Product**

SCM

**Privilege**

Administrator

**Syntax**

```
cscf translation { default | name list_name [ -noconfirm ] }

no cscf translation name list_name
```

- **default**
  Specifies that the system is to enter the Translation Configuration Mode for the default translation list.

- **name list_name**
  Specifies a name for the translation list.
  `list_name` must be from 1 to 79 alpha and/or numeric characters in length.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create a new translation list and enter the Translation Configuration Mode or enter the mode for an existing list.

Translation lists are used to modify or replace a request-URI such as an E.164 number. For example, a translation list can be configured to append digits to the end of a number or replace a domain name with another.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-translation)#
```

Translation Configuration Mode commands are defined in the *CSCF Translation Configuration Mode Commands* chapter.

Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

**Example**

The following command enters the Translation Configuration Mode for a translation list named `trans_list3`:

```
cscf translation name trans_list3
```
cscf urn-service-list

Creates/removes a URN service list and/or enters the URN List Configuration Mode.

Product  
SCM

Privilege  
Administrator

Syntax

cscf urn-service-list { default | name list_name [ -noconfirm ] }

no cscf urn-service-list name list_name

---

**cscf urn-service-list**

- **default**  
  Specifies that the system is to enter the URN List Configuration Mode for the default URN service list.

- **name list_name**  
  Specifies a name for the URN service list.  
  `list_name` must be from 1 to 79 alpha and/or numeric characters.

- **-noconfirm**  
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create a URN service list name and enter the URN List Configuration Mode. URN lists contain URN to URI mappings used for emergency and location-based services. A URN service list is selected by a CSCF session template.  
Entering this command results in the following prompt:  
```
[context_name]hostname(config-cscf-service-urn)#
```
URN List Configuration Mode commands are defined in the **CSCF URN List Configuration Mode Commands** chapter.  
Use this command when configuring the following SCM components: P-CSCF.

**Example**

The following command enters the URN List Configuration Mode for a URN list named `urn_list1`:

```
cscf urn-service-list name urn_list1
```
css server

This is a restricted command. In Release 9.0 and later, this command is obsoleted.
default aaa

Restores the system’s accounting and authentication parameters to default settings for the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
default aaa { accounting { administrator | subscriber } | authentication { administrator | subscriber }
```

```
accounting { administrator | subscriber }
administrator: Restores the system default setting for RADIUS accounting for administrative user sessions.
subscriber: Restores the system default setting for RADIUS accounting for subscriber sessions.

authentication { administrator | subscriber }
subscriber: Restores the system default setting for RADIUS authentication for subscribers.
administrator: Restores the system default setting for RADIUS authentication for administrative users.
```

Usage
Use this command to restore the system’s accounting and authentication options to the default settings for the current context.
The system is shipped from the factory with the administrative user and subscriber RADIUS accounting enabled.

Example

```
default aaa accounting subscriber
default aaa authentication default
```
default access-list

Restores the system default for packet handling when an undefined ACL is specified.

**Product**
- PDSN, FA, HA, GGSN

**Privilege**
- Security Administrator, Administrator

**Syntax**
```
default access-list undefined
```

**Usage**
Restores the system default for handling of packets when an undefined ACL is specified.

**Example**
```
default access-list undefined
```
default gtpp

Restores gtpp parameter settings to their default values.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

default gtpp { attribute { diagnostics | duration-ms | local-record-sequence-number | plmn-id } | algorithm | deadtime | detect-dead-server { consecutive-failures } | duplicate-hold-time | echo-interval | egcdr final-record { include-content-ids only-with-traffic closing-cause same-in-all-partials } | egcdr losdv-max-containers | egcdr lotdv-max-containers | egcdr service-idle-timeout | max-cdrs | max-pdu-size | max-retries | redirection-allowed | timeout | trigger}

attribute { diagnostics | duration-ms | local-record-sequence-number | plmn-id }
Restores the gtpp attribute parameter to the following default settings:
- **diagnostics**: Disabled
- **duration-ms**: Disabled
- **local-record-sequence-number**: Disabled
- **plmn-id**: Enabled

algorithm
Restores the gtpp algorithm parameter to its default setting of first-server.

deadtime
Restores the gtpp deadtime parameter to its default setting of 120 seconds.

detect-dead-server { consecutive-failures }
Restores the gtpp detect-dead-server consecutive-failure parameter to its default setting of 5.

duplicate-hold-time
Restores the gtpp duplicate-hold-time parameter to its default setting of 60 minutes.

echo-interval
Restores the gtpp echo-interval parameter to its default setting of 60 seconds.
After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

**Example**
The following command restores the gtp max-pdu-size to its default setting of 4096 octets:

```
default gtp max-pdu-size
```
Context Configuration Mode Commands

default gtpv
**default mobile-ip**

Sets the behavior of all HA services when a new call has a duplicate home address or IMSI.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
defaultmobile-ip { hanewcall { duplicate-home-address | duplicate-imsi-session } | fa { multiple-dynamic-reg-per-nai | newcallduplicate-home-address } }
```

- **duplicate-home-address**
  
  Set HA or FA services to reject a new call that requests an IP address that is already assigned.

- **duplicate-imsi-session**
  
  Set HA services to accept new calls that have the same IMSI as a call that is already active.

- **multiple-dynamic-reg-per-nai**
  
  All FA services in the current context can not simultaneously setup multiple dynamic home address registrations that have the same NAI.

**Usage**

Use this command to reset the HA behavior for new calls.

**Example**

The following commands reset the HA and the FA to reject new calls that request a static IP address that is already in use from an IP pool in the same destination context:

```plaintext
default mobile-ip ha newcall duplicate-home-address

default mobile-ip fa newcall duplicate-home-address
```
**default network-requested-pdp-context**

Restores network-requested-pdp-context parameters to their default settings.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default network-requested-pdp-context { hold-down-time | sgsn-cache-time }
```

- **hold-down-time**
  Restores the hold-down-time parameter to its default setting of 60 seconds.

- **sgsn-cache-time**
  Restores the sgsn-cache-time parameter to its default setting of 300 seconds.

**Usage**

After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

**Example**

The following command restores the network-requested-pdp-context hold-down-time parameter to its default setting:

```
default network-requested-pdp-context hold-down-time
```
default ppp

Restores the point-to-point protocol option defaults.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
```

**acfc { receive | transmit }

*receive*: Set the ACFC receive setting to the default, allow. The local PPP side indicates that it can process ACFC compressed PPP packets and compressed packets are allowed.

*transmit*: Set the ACFC transmit setting to the default, ignore. If the peer requests ACFC, the request is accepted, but ACFC is not applied for transmitted PPP packets.

**auth-retry suppress-aaa-auth

Restores the system default and allows authentication retries to the AAA server after authorization has already been performed.

**chap fixed-challenge-length

Disables a specified fixed PPP CHAP challenge length and sets the system back to the default of a random PPP CHAP challenge length from 17 to 32 bytes.

**echo-max-retransmissions

Restores the system default for the maximum number of retransmissions of LCP ECHO_REQ before a session is terminated in an always-on session.

**echo-retransmit-timeout

Restores the system default for the timeout before trying LCP ECHO_REQ for an always-on session.

**first-lcp-retransmit-timeout

Sets the number of milliseconds to wait before the first retransmit of a control packet. to the system default.

**lcp-authentication-reject retry-alternate

Default: Disabled. No alternate authentication option will be retried.
The action that is taken if the authentication option is rejected during LCP negotiation and retry the allowed alternate authentication option

```
lcp start-delay
```
Sets the delay before Line Control Protocol (LCP) starts to it’s default of 0 (zero) milliseconds.

```
lcp-terminate connect-state
```
This option enables sending an LCP terminate message to the Mobile Node when a PPP session is disconnected if the PPP session was already in a connected state.
Note that if the no keyword is used with this option, the PDSN must still send LCP Terminate in the event of an LCP/PCP negotiation failure or PPP authentication failure, which happens during connecting state.

**Important:** This option is not supported in conjunction with the GGSN product.

```
lcp-terminate mip-lifetime-expiry
```
This option configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to MIP Lifetime expiry (default).
Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to MIP Lifetime expiry.

```
lcp-terminate mip-revocation
```
This option configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to a Revocation being received from the HA (default).
Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to a Revocation being received from the HA.

```
max-authentication-attempts
```
Restores the maximum PPP authentication retry attempts possible from the peer, when the authentication attempts fail to the default of 1.

```
max-configuration-nak
```
Restores the maximum number of consecutive configuration NAKs to be sent to the peer before disconnecting the PPP session to the default of 10.

```
max-retransmissions
```
Restores the system default for the maximum number of times to retransmit control packets.

```
max-terminate
```
Restore the maximum number of PPP LCP Terminate Requests transmitted to the Mobile Node to the system default of 2.

```
mru
```
Resets the maximum packet size than can be received to the default of 1500.
negotiate default-value-options
Disables the inclusion of configuration options with default values in PPP configuration requests.

peer-authentication
Sets the peer authentication user name and password to its system default.

pfc { receive | transmit }
**receive**: Sets the Protocol Field Compression (PFC) receive setting to the default, allow. The peer is allowed to request PFC during LCP negotiation.
**transmit**: Sets the PFC transmit setting to the default, ignore. If the peer requests PFC, it is accepted but PFC is not applied for transmitted packets.

reject-peer-authentication
Rejection of peer requests for authentication is enabled.

renegotiation retain-ip-address
Retain the currently allocated IP address for the session during PPP renegotiation (Simple IP) between FA and Mobile node.

retransmit-timeout
Restores the number of milliseconds to wait before retransmitting packets.

Usage
Restore the PPP settings for the current context to the system defaults.

Example

default ppp echo-max-retransmissions
default ppp echo-retransmit-timeout
default ppp max-retransmissions
default ppp peer-authentication
default ppp retransmit-timeout
**default radius**

This command restores the context’s RADIUS parameters to the system default settings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default radius { accounting { algorithm | deadtime | detect-dead-server consecutive-failures | max-outstanding | max-pdu-size | max-retries | timeout } | algorithm | attribute { nas-identifier } | deadtime | detect-dead-server consecutive-failures | dictionary | keepalive | max-outstanding | max-retries | max-transmissions | probe-interval | timeout }
```

Restores the system default value for the RADIUS accounting option specified.
- `algorithm`: restores the accounting server selection algorithm to the system default.
- `apn-to-be-included`: configures the APN name to be included for radius accounting.
- `archive`: enables archiving of RADIUS accounting messages.
- `deadtime`: restores the default number of seconds before attempting to communicate an accounting server marked as unreachable.
- `detect-dead-server consecutive-failures`: restores the default value for the number of consecutive failed attempts to reach an accounting server before it is marked as unreachable.
- `radius-accounting-policy`: resets the HA accounting policy to the system default: session-start-stop. Send Accounting Start when the Session is connected, Send Accounting Stop when the session is disconnected.
- `keepalive`: restores the default keepalive accounting related parameters values.
- `max-outstanding`: restores the system default for the maximum number of outstanding messages to queue for a given accounting server.
- `max-pdu-size`: restores the maximum size a packet data unit can be.
- `max-retries`: restores the maximum number of times a packet will be retransmitted to the system default.
- `max-transmissions`: disables the maximum transmissions limit.
- `rp trigger-policy`: restores the RADIUS accounting R-P policy to the default of Airlink Usage.
- `timeout`: restores the number of seconds to wait before retransmitting a PDU to the system default.

```
algorithm
```

Restores the RADIUS server selection algorithm to the system default.

```
attribute { nas-identifier }
```

- `nas-identifier`: restores the network access server Id to the system default.
deadtime
Restores the default number of seconds before attempting to communicate an RADIUS server marked as unreachable.

detect-dead-server
Restores consecutive failures to the default of 4 and disables response-timeout.

dictionary
Restores the context’s dictionary to the system default.

keepalive [ calling-station-id id | consecutive-response number | encrypted | interval seconds | password | retries number | timeout seconds | username name | valid-response access-accept [ access-reject ] ]
calling-station-id id: restores the default calling-station-id to be used for the keepalive authentication.
consecutive-response number: restores the default number of consecutive authentication responses after which the server is marked as reachable.
interval seconds: restores the default time interval between the keepalive authentication requests.
password: restores the default password to be used for the authentication.
retries number: restores the default number of times the keepalive access request to be sent before marking the server as unreachable.
timeout seconds: restores the default time interval between each keepalive access request retries.
username name: restores the default username to be used for the authentication.
valid-response access-accept [ access-reject]: restores the default valid response for the authentication request.

max-outstanding
Restores the system default for the maximum number of outstanding messages to queue for a given RADIUS server.

max-retries
Restores the maximum number of times a packet will be retransmitted to the system default.

probe-interval
Sets the amount of time to wait before sending another probe authentication request to a RADIUS server to the default setting of 60 seconds.

timeout
Restores the number of seconds to wait before retransmitting a message to the system default.

Usage
Restores RADIUS parameters to the system default settings.

Example
default radius accounting deadtime
default radius accounting max-outstanding
default radius algorithm
default radius attribute nas-identifier
default radius authenticate null-username

Restores the system default for authenticating null, or blank, user names. The default behavior is to authenticate, send Access-Request messages to the AAA server, all user names including null user names.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

default radius authenticate null-username

Usage

Use this command to return to the default behavior of authenticating, sending Access-Request messages to the AAA server, all user names, including NULL user names.

Example

Enter the following command to return username authentication to the default behavior:

default radius authenticate null-username
default threshold

Restores context-level thresholds to their default settings.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
default threshold { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-pool-release | ip-pool-used | monitoring available-ip-pool-group }
```

**available-ip-pool-group**
Restores the context-level IP address pool group utilization thresholds to their default values.

**ip-pool-free**
Default: 0
Restores to it’s default the thresholds for the percentage of the IP pool addresses that are in the free state.

**ip-pool-hold**
Default: 0
Restores to it’s default the thresholds for the percentage of the IP pool addresses that are in the hold state.

**ip-pool-release**
Default: 0
Restores to it’s default the thresholds for the percentage of IP pool address that are in the release state.

**ip-pool-used**
Default: 0
Restores to it’s default the thresholds for the percentage off the IP pool addresses that are used.

**monitoring available-ip-pool-group**
Restores the IP address pool threshold monitoring parameter to its default setting.

Usage
Use this command to restore IP address pool-related threshold parameters to their default settings.

Example

```
default threshold available-ip-pool-group
```
dhcp-service

Adds a Dynamic Host Control Protocol (DHCP) service instance to the current context and enters the configuration mode for that service.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

dhcp-service service_name

no dhcp-service service_name

no
Removes a previously configured DHCP service from the current context.

service_name
The name by which the DHCP service is to be recognized by the system. The name can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.

Usage
Use this command to add a DHCP service to a context configured on the system and enter the DHCP service configuration mode. A DHCP service is a logical grouping of external DHCP servers. The DHCP configuration mode provides parameters that dictate the system’s communication with one or more of these DHCP servers. A maximum of 256 services (regardless of type) can be configured per system.

⚠️ Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the DHCP Service Configuration Mode chapter of this reference for additional information.

Example
The following command creates a DHCP service called DHCP1 and enter the DHCP service configuration mode:

```sh
dhcp-service dhcp1
```
diameter accounting

This command configures Diameter accounting related settings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq | rf-plus } | endpoint endpoint_name | hd-mode | fall-back-to-local | hd-storage-policy hd_policy | max-retries tries | max-transmissions transmissions | request-timeout duration | server host_name | priority priority }
```

**default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }

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

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

- **endpoint**: Removes the currently configured accounting endpoint. The default accounting server configured in the default AAA group will be used.
- **hd-mode**: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.
- **hd-storage-policy**: Disables use of the specified HD storage policy.
- **max-retries**: Disables the retry attempts for Diameter accounting in this AAA group.
- **max-transmissions**: Disables the maximum number of transmission attempts for Diameter accounting in this AAA group.
- **server host_name**: Removes the Diameter host host_name from this AAA server group for Diameter accounting.

**default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }

- **dictionary**: Sets the context’s dictionary as the system default.
- **hd-mode**: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.
- **max-retries**: Sets the retry attempts for Diameter accounting in this AAA group to default 0 (disable).
- **max-transmissions**: Sets the maximum transmission attempts for Diameter accounting in this AAA group to default 0 (disable).
- **request-timeout**: Sets the timeout duration, in seconds, for Diameter accounting requests in this AAA group to default (20).
Context Configuration Mode Commands

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

Specifies the Diameter accounting dictionary.

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

**nasreq**: nasreq dictionary—the dictionary defined by RFC 4005.

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

```plaintext
diameter accounting
```

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

**endpoint_name** must be a string of 1 through 63 characters in length.

### HD Storage Policies

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

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

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

Specifies the HD Storage policy name.

**hd_policy** must be the name of a configured HD Storage policy, and must be a string of 1 through 63 alpha and/or numeric characters in length.

HD storage policies are configured through the Global Configuration Mode.

This and the **hd-mode** command are used to enable the storage of Rf Diameter Messages to HDD in case all Diameter Servers are down or unreachable.

```plaintext
max-retries tries
```

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

**tries** specifies the maximum number of retry attempts. The value must be an integer from 1 through 1000. Default: 0

```plaintext
max-transmissions transmissions
```

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

**transmissions** specifies the maximum number of transmission attempts for a Diameter request. The value must be an integer from 1 through 1000. Default: 0

```plaintext
request-timeout duration
```

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.

**duration** specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request. The value must be an integer from 1 to 3600. Default: 20

```plaintext
server host_name priority priority
```

Specifies the current context Diameter accounting server’s host name and priority.
host_name specifies the Diameter host name, it must be a string of 1 through 63 characters in length.

priority specifies the relative priority of this Diameter host. The priority is used in server selection. The priority must be an integer from 1 through 1000.

Usage

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

Example

The following command specifies the Diameter accounting dictionary:

diameter accounting dictionary <dictionary>

The following command specifies the Diameter endpoint:

diameter accounting endpoint <endpoint_name>

The following commands specify the Diameter accounting options:

diameter accounting max-retries <tries>
diameter accounting max-transmissions <transmissions>
diameter accounting request-timeout <duration>
diameter accounting server <host_name> priority <priority>

The following commands disable/clear the options:

no diameter accounting endpoint
no diameter accounting server <host_name>
diameter authentication

Use this command to configure Diameter authentication related settings.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter authentication { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq } | endpoint endpoint_name | max-retries tries | max-transmissions transmissions | redirect-host-avp { just-primary | primary-then-secondary } | request-timeout duration | server host_name priority priority }

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

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

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

endpoint: Removes the authentication endpoint. The default server configured in default AAA group will be used.
max-retries: Disables the retry attempts for Diameter authentication in this AAA group.
max-transmissions: Disables the maximum transmission attempts for Diameter authentication in this AAA group.
server host_name: Removes the Diameter host host_name from this AAA server group for Diameter authentication.

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

dictionary: Sets the context’s dictionary as the system default.
max-retries: Sets the retry attempts for Diameter authentication requests in this AAA group to default 0 (disable).
max-transmissions: Sets the configured maximum transmission attempts for Diameter authentication in this AAA group to default 0 (disable).
redirect-host-avp: Sets the redirect choice to default (just-primary).
request-timeout: Sets the timeout duration, in seconds, for Diameter authentication requests in this AAA group to default (20).

Specifies the Diameter authentication dictionary.

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

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

**nasreq** nasreq dictionary—the dictionary defined by RFC 4005.

**endpoint endpoint_name**

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

**max-retries tries**

Specifies how many times a Diameter authentication request should be retried with the same server, if the server fails to respond to a request. tries specifies the maximum number of retry attempts, and must be an integer from 1 through 1000. Default: 0

**max-transmissions transmissions**

Specifies the maximum number of transmission attempts for a Diameter authentication request. Use this in conjunction with the "max-retries tries" option to control how many servers will be attempted to communicate with. transmissions specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000. Default: 0

**diameter authentication redirect-host-avp { just-primary | primary-then-secondary }**

Specifies whether to use just one returned AVP, or use the first returned AVP as selecting the primary host and the second returned AVP as selecting the secondary host.

**just-primary:** Redirect only to primary host.

**primary-then-secondary:** Redirect to primary host, if fails then redirect to the secondary host. Default: just-primary

**request-timeout duration**

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.

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

**server host_name priority priority**

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

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

Example
The following command specifies the Diameter authentication dictionary:

diameter authentication dictionary <dictionary>
The following command specifies the Diameter endpoint:

diameter authentication endpoint <endpoint_name>
The following commands specify Diameter authentication options:

diameter authentication max-retries <tries>
diameter authentication max-transmissions <transmissions>
diameter authentication redirect-host-avp primary-then-secondary
diameter authentication server <host_name> priority <priority>
diameter authentication request-timeout <duration>
The following commands disable/clear the options:

no diameter authentication endpoint
no diameter authentication server <host_name>
diameter authentication failure-handling

This command configures error handling for Diameter EAP requests.

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

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

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

---

```plaintext
no
Disables Diameter authentication failure handling.

default
Configures the default Diameter authentication failure handling setting.

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

eap-request
Specifies configuring failure handling for EAP requests.

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

request-timeout action { continue | retry-and-terminate | terminate }
Specifies the action to be taken for failures:
- `continue`: Continues the session
- `retry-and-terminate`: First retries, if it fails then terminates the session
- `terminate`: Terminates the session

result-code result_code { [ to result_code ] action { continue | retry-and-terminate | terminate } }
`result_code` specifies the result code number, must be an integer from 1 through 65535.
diameter authentication failure-handling

**to result_code**: Specifies the upper limit of a range of result codes. to result_code must be greater than result_code.

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

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

**Usage**

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

**Example**

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

```
diameter authentication failure-handling eap-request result-code 5001 to 5005 action continue

diameter authentication failure-handling eap-request result-code 5003 action terminate
```
diameter dictionary

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

This command enables creating/configuring/deleting a Diameter endpoint.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
diameter endpoint  endpoint_name  [ -noconfirm ]
no diameter endpoint  endpoint_name
```

---

**no**
Removes the specified Diameter endpoint.

---

**endpoint_name**
Specifies the Diameter endpoint name.
- `endpoint_name` must be an alpha and/or numeric string of 1 through 63 characters in length.
- If the named endpoint does not exist, it is created, and the CLI mode changes to the Diameter Endpoint Configuration mode wherein the endpoint can be configured.
- If the named endpoint already exists, the CLI mode changes to the Diameter Endpoint Configuration mode wherein the endpoint can be reconfigured.

---

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

---

**Usage**
Use this command to create/configure/delete a Diameter origin endpoint.

---

**Example**
The following command creates a Diameter origin endpoint named `test13`:

```
diameter endpoint  test13
```
diameter sctp

Configures Diameter SCTP parameters for all diameter endpoints within the context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
diameter sctp { heartbeat-interval interval | path max-retransmissions retransmissions } 
```

default diameter sctp { heartbeat-interval | path max-retransmissions }

- **default**
  
  Configures this command with the default settings.

- **heartbeat-interval**
  
  Sets the heartbeat interval to the default value.

- **path max-retransmissions**
  
  Sets the SCTP path maximum retransmissions to the default value.

- **heartbeat-interval interval**
  
  Specifies the time interval between heartbeat chunks sent to a destination transport address in seconds. `interval` must be an integer from 1 through 255.

  Default: 30 seconds

- **path max-retransmissions retransmissions**
  
  Specifies the maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive.

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

  Default: 10

**Usage**

Use this command to configure Diameter SCTP parameters for all diameter endpoints within the context.

**Example**

The following command configures the heartbeat interval to 60 seconds:

```
diameter sctp heartbeat-interval 60
```

The following command configures the maximum number of consecutive retransmissions to 6, after which the endpoint is marked as inactive:

```
diameter sctp path max-retransmissions 6
```
diameter origin

This command is deprecated and is replaced by the `diameter endpoint` command.
dns-client

Creates a DNS client and/or enters the DNS Client Configuration Mode.

Product
SCM, SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] dns-client name [ -noconfirm ]

no
Removes the specified DNS client from the context.

name
Specifies a name for the DNS client. name must be from 1 to 63 alpha and/or numeric characters in length.

Usage
Use this command to create a new DNS client and enter the DNS Client Configuration Mode or enter the mode for an existing client.
Entering this command results in the following prompt:
[context_name]hostname(config-dns-client)#
DNS Client Configuration Mode commands are defined in the DNS Client Configuration Mode Commands chapter.

Example
The following command enters the DNS Client Configuration Mode for a DNS client named dns1:

dns-client dns1
**domain**

Configures a domain alias for the current context.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
domain [ * ] domain_name [ default subscriber subs_temp_name ]
no domain [ * ] domain_name
```

- **no domain [ * ] domain_name**
  
  Indicates the domain specified is to be removed as an alias to the current context.

- **[ * ] domain_name**
  
  `domain_name` specifies the domain alias to create/remove from the current context. If the domain portion of a subscriber’s user name matches this value, the current context is used for that subscriber.

  `domain_name` must be an alpha and/or numeric string of 1 through 79 characters in length. The domain name can contain all special characters, however note that the character * (wildcard character) is only allowed at the beginning of the domain name.

  If the domain name is prefixed with * (wildcard character), and an exact match is not found for the domain portion of a subscriber’s user name, subdomains of the domain name are matched. For example, if the domain portion of a subscriber’s user name is abc.xyz.com and you use the domain command `domain *xyz.com` it matches. But if you do not use the wildcard (`domain xyz.com`) it does not match.

- **Important:** The domain alias specified must not conflict with the name of any existing context or domain names.

- **default subscriber subs_temp_name**
  
  Specifies the name of the subscriber template to apply to subscribers using this domain alias.

  `subs_temp_name` must be an alpha and/or numeric string of 1 through 127 characters in length. If this keyword is not specified the default subscriber configuration in the current context is used.

**Usage**

Set a domain alias when a single context may be used to support multiple domains via aliasing.

**Example**

```plaintext
domain sampleDomain.net
no domain sampleDomain.net
```
**eap-profile**

Creates a new, or specifies an existing, Extensible Authentication Protocol (EAP) profile and enters the EAP Configuration Mode.

**Product**
ASN GW, PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] eap-profile name
```

`name`
Specifies the name of a new or existing EAP profile. `name` must be from 1 to 256 alpha and/or numeric characters.

**Usage**

Use this command to create a new or enter an existing EAP profile. Entering this command results in the following prompt:

```
[context_name]hostname(config-ctx-eap-profile)#
```

EAP Configuration Mode commands are defined in the EAP Configuration Mode Commands chapter.

**Example**
The following command configures an EAP profile called `eap1` and enters the EAP Configuration Mode:

```
eap-profile eap1
```
edr-module active-charging-service

This command creates the Event Data Record (EDR) module and enters the EDR Module Active Charging Service Configuration Mode.

Product
ACS, GGSN, HA, LNS, PDSN

Privilege
Security Administrator, Administrator

Syntax

edr-module active-charging-service

Usage
Use this command to create the EDR module for the context and configure the EDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the UDR module command.

Example

edr-module active-charging-service
egtp-service

Creates an eGTP service or specifies an existing eGTP service and enters the eGTP service configuration mode for the current context.

Product
MME, P-GW, S-GW

Privilege
Administrator

Syntax

```
egtp-service service_name [-noconfirm ]
```

```
no egtp-service service_name
```

**service_name**
Specifies the name of the eGTP service. If `service_name` does not refer to an existing service, the new service is created if resources allow.
```
service_name must be from 1 to 63 alpha and/or numeric characters.
```

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

```
no egtp-service service_name
```

Removes the specified eGTP service from the context.

Usage

Enter the eGTP service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
```
A maximum of 256 services (regardless of type) can be configured per system.
```

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:
```
[context_name]hostname(config-egtp-service)#
```

eGTP Service Configuration Mode commands are defined in the eGTP Service Configuration Mode Commands chapter.
```
Use this command when configuring the following GTP SAE components: MME, P-GW, and S-GW.
```

**Example**

The following command enters the existing eGTP service configuration mode (or creates it if it doesn’t already exist) for the service named `egtp-service1`:
egtp-service egtp-service1

The following command will remove egtp-service1 from the system:

no egtp-service egtp-service1
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
**exit**

Exits the context configuration mode and returns to the global configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the Global Configuration mode.
external-inline-server

This is a restricted command.
**fa-service**

Creates/deletes a foreign agent service or specifies an existing FA service for which to enter the foreign agent service configuration mode for the current context.

**Product**

PDSN, ASN-GW, FA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] fa-service name
```

- **name**
  Specifies the name of the FA service to configure. If `name` does not refer to an existing service, the new service is created if resources allow. `name` must be from 1 to 63 alpha and/or numeric characters.

- **no**
  Indicates the foreign agent service specified is to be removed.

**Usage**

Enter the FA service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

⚠️ **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

**Example**

The following command will enter the FA service configuration mode creating the service `sampleService`, if necessary.

```
fa-service sampleService
```

The following command will remove `sampleService` as being a defined FA service.

```
no fa-service sampleService
```
firewall max-associations

This command is obsolete.
ggsn-service

Creates/deletes a Gateway GPRS Support Node (GGSN) service and enters the GGSN service configuration mode within the current context.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ggsn-service name [-noconfirm ]
```

**no ggsn-service name**

**no**
Deletes a previously configured GGSN service.

**name**
Specifies the name of the GGSN service to create/configure. *name* must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**
Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as a GGSN in a GPRS or UMTS network. This command is also used to remove previously configured GGSN services. A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

**Example**
The following command creates a GGSN service name ggsn1:

```
ggsn-service ggsn1
```
gprs-service

This command creates a GPRS service instance and enters the GPRS Service configuration mode. This mode configures all of the parameters specific to the operation of an SGSN in a GPRS network.

**Important:** For details about the commands and parameters for this mode, check the GPRS Service Configuration Mode chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gprs-service srvc_name

no gprs-service srvc_name
```

- **no**
  Remove the configuration for the specified IGPRS service from the configuration for the current context.

  **srvc_name**
  A unique string of 1 to 63 alphanumeric characters that identify the specific GPRS service.

**Usage**

Use this command to create or remove a GPRS service. Entering this command will move the system to the GPRS Service configuration mode and change the prompt to:

```
[context_name]hostname(config-gprs-service)#
```

**Example**
The following command creates a GPRS service named gprs1:

```
gprs-service gprs1
```

The following command removes the GPRS service named gprs1:

```
no gprs-service gprs1
```
gs-service

This command creates a Gs service instance and enters the Gs Service configuration mode. This mode configures the parameters specific to the Gs interface between the SGSN and the MSC/VLR.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
gs-service svc_name [-noconfirm ]
```

```bash
no gs-service svc_name
```

- **no**
  Remove the configured Gs service from the current context.

- **svc_name**
  A unique string of 1 to 63 alphanumeric characters that identify the specific Gs service.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create, edit, or remove a Gs service.

A maximum of 32 Gs service can be configured in one context/system. This limit is subject to maximum of 256 services (regardless of type) can be configured per system.

**Important:** For details about the commands and parameters for this mode, refer Gs Service Configuration Mode chapter.

**Example**

The following command creates an Gs service named ‘gs1’:

```bash
gs-service gs1
```

The following command removes the Gs service named ‘gs1’:

```bash
no gs-service gs1
```
gtpp

The commands in this section change gtpp related parameters.
gtpp algorithm

Configures GTPP routing algorithms for the current context.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp algorithm { first-server | round-robin | first-n n }

- **first-server**
  Default: Enabled
  Specifies that accounting data is sent to the first available charging gateway function (CGF) based upon the relative priority of each configured CGF.

- **round-robin**
  Default: Disabled
  Specifies that accounting data is transmitted in a circular queue fashion such that data is sent to the highest priority CGF first, then to the next available CGF of the highest priority, and so on. Ultimately, the queue returns to the CGF with the highest configured priority.

- **first-n n**
  Default: 1 (Disabled)
  Specifies that the AGW must send accounting data to $n$ (more than one) CGFs based on their priority.
  Response from any one of the $n$ CGFs would suffice to proceed with the call. The full set of accounting data is sent to each of the $n$ CGFs.
  $n$ is the number of CGFs to which accounting data will be sent, and must be an integer from 2 through 65535.

Usage
Use this command to control how G-CDR accounting data is routed among the configured CGFs.

Example
The following command configures the system to use the round-robin algorithm when transmitting G-CDR accounting data:

```
gtpp algorithm round-robin
```
gtpp attribute

This command allows the specification of the optional attributes to be present in the call detail records (CDRs) that the GPRS/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | node-id-suffix suffix | plmn-id [ unknown-use uncode_value ] | rat | record-extensions rat | sms { destination-number | recording-entity | service-centre } }

[ default ] gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | plmn-id | rat | record-extensions | sms { destination-number | recording-entity | service-centre } }

[ no ] gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | node-id-suffix | plmn-id | rat | record-extensions rat | sms { destination-number | recording-entity | service-centre } }

no
Removes the configured GTPP attributes from the CDRs.

default
Sets the default GTPP attributes in generated the CDRs. It also sets the default presentation of attribute values in generated CDRs.

cell-plmn-id
Default: Disabled
This keyword configures the SGSN to include the cell’s PLMN identifier (MCC and MNC) in generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

diagnostics
Default: Disabled
Includes the Diagnostic field in the CDR that is created when PDP contexts are released. The field will contain one of the following values:
- **36** - if the SGSN sends us "delete PDP context request".
- **38** - if the GGSN sends "delete PDP context request" due to GTP-C/GTP-U echo timeout with SGSN.
- **40** - if the GGSN sends "delete PDP context request" due to receiving a RADIUS Disconnect-Request message.
• **26** - if the GGSN sends "delete PDP context request" for any other reason (e.g., the operator types "clear subscribers" on the GGSN).

**duration-ms**
Default: Disabled
Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require).

**imei**
Default: Disabled
This keyword configures the SGSN to include the International Mobile Equipment Id in generated CDRs (M-CDRs and/or the S-CDRs). This keyword is applicable for SGSN only.

**local-record-sequence-number**
Default: Disabled
Includes the Node ID field in the CDR that is created when PDP contexts are released. The field consists of a AAA Manager identifier automatically appended to the name of the GGSN or SGSN service. The name of the GGSN/SGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.

**msisdn**
Default: Disabled
This keyword configures the SGSN to include the Mobile Subscribers Integrated Services Digital Network identifier in generated CDRs (M-CDRs and/or the S-CDRs). This keyword is applicable for SGSN only.

**node-id-suffix string**
Default: Disabled
Specifies the string suffix to use in the NodeID field of GTPP CDRs. Each Session Manager task generates a unique NodeID string per GTPP context.

*string:* This is the configured Node-ID-Suffix having any string between 1 to 16 characters.

**Important:** The NodeID field is a printable string of the ndddstring format: n: The first digit is the SessMgr restart counter having a value between 0 and 7. ddd: The number of SessMgr instances. Uses the specified NodeID-suffix in all CDRs. The “Node-ID” field is consists of SessMgr Recovery counter (1 digit) n + AAA Manager identifier (3 digits) ddd + the configured Node-Id-suffix (1 to 16 characters) string.

**Important:** If the centralized LRSN feature is enabled, the “Node-ID” field consists of only the specified NodeID-suffix. Otherwise GTPP group name is used. For default GTPP groups, GTPP context-name (truncated to 16 characters) is used.

**Important:** SessMgr recovery counter gets updated in case of “session recovery not enabled” If session recovery is enabled, the counter never updates. The node-id is displayed in the G-CDR irrespective of gtpp dictionary. The G-CDR is not decoded in monitor protocol for custom1 / custom3 dictionaries.
plmn-id [ unknown-use uncode_value ]

Default: Enabled
Includes the SGSN PLMN Identifier value (the RAI) in generated CDR (M-CDRs and/or the S-CDRs), if it is provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.

**Important:** For the GGSN it provides radio access identifier as the SGSN PLMN Id and for SGSN it includes the PLMN-id of RNC.

unknown-use uncode_value encodes the specified value for "SGSN PLMN Identifier" in the CDR if SGSN PLMN-ID information is unavailable.
Must be followed by the uncode_value value to be encoded.
uncode_value must be an hexadecimal value between 0x0 and 0xFFFFFF.
This keyword is applicable for SGSN only.

rat

Default: Disabled
This keyword configures the SGSN to include the radio access technology attribute in generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

record-extensions rat

Default: Disabled
This keyword configures the SGSN to include the radio access technology attribute in record extension field of generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

sms { destination-number | recording-entity | service-centre }

Default: Disabled
This keyword configures the SGSN to include the SMS related attributes in generated S-SMO-CDRs or S-SMT-CDRs.
destination-number: This keyword includes the destination-number information of SMS in generated S-SMO-CDRs or S-SMT-CDRs.
Note: This is the destination number of the short message subscriber.
recording-entity: This keyword includes the recording entity information of SMS in generated S-SMO-CDRs or S-SMT-CDRs.
Note: The recording entity is the E.164 number of the SGSN.
service-centre: This keyword includes the service-centre information of SMS in generated S-SMO-CDRs or S-SMT-CDRs.
Note: This is the E.164 address of the SMS-service centre.
This keyword is applicable for SGSN only.

Usage

Use this command to configure the type of optional information fields to include in generated CDRs (M-CDRs, S-CDRs, S-SMO-CDR, S-SMT-CDR from SGSN and G-CDRs, eG-CDRs from GGSN) by the AGW (SGSN and/or GGSN). In addition, it controls how the information for some of the mandatory fields are reported. Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).
**Important:** This command can be repeated multiple times with different keywords to configure multiple GTPP attributes.

**Example**
The following command configures the system to present the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```
gtpp charging-agent

Configures the IP address and port of the system interface within the current context used to communicate with the CGF.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp charging-agent address ip_address [port port]
```

- `no gtpp charging-agent`
  - `no`
    - Removes a previously configured charging agent address.
  - `address ip_address`
    - Specifies the IP address of the interface configured within the current context that is used to transmit CDR records (G-CDR/eGCRD/M-CDR/S-CDR) to the CGF.
    - `ip_address` must be configured using dotted decimal notation.
  - `port port`
    - It is an optional parameter. It specifies the Charging Agent UDP port.
    - If `port` is not defined IP will take default port number 49999.
    - `port` is a port number. Must be followed by an integer, ranging from 1 to 65535.

**Important:** Configuring `gtpp charging-agent` on port 3386 may interfere with `ggsn-service` configured with the same `ip address`.

- Default: 49999

**Usage**

This command establishes a Ga interface for the system. For GTPP accounting, one or more Ga interfaces must be specified for communication with the CGF. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the `gtpp` commands in this chapter).

This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GSN is known to the CGF. Therefore, the IP address used for the Ga interface could be identical to one bound to a GSN service (a Gn interface).

If no GSN service is configured in the same context as the Ga interface, the address configured by this command is used to receive unsolicited GTPP packets.

**Example**

---

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01
The following command configures the system to use the interface with an IP address of 192.168.13.10 as the accounting interface with port 20000 to the CGF:

```
gtp charging-agent address 192.168.13.10

gtp charging-agent address 192.168.13.10 port 20000
```
**Context Configuration Mode Commands**

**gtpp data-request sequence-numbers**

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp data-request sequence-numbers start { 0 | 1 }
default gtpp data-request sequence-numbers start
```

- **default**
  Default is 0 (zero).

- **start**
  Specifies the value of the start sequence number for the GTPP Data Record Transfer Request. Default: 0
  - 0 = Designates the start sequence number as 0.
  - 1 = Designates the start sequence number as 1.

**Usage**

When the GGSN/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that can not properly handle the re-use of sequence number 0 in the echo request packets.

**Example**

The following command sets the sequence to start at 1.

```
gtpp data-request sequence-numbers start 1
```
gtpp dead-server suppress-cdrs

This command enables/disables CDR archival when a dead server is detected.

**Important:** This command is customer specific. For more information please contact your local service representative.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] gtpp dead-server suppress-cdrs
```

- **default**
  Configures the default setting.
  Default: Disabled

- **no**
  Disables CDR archival.

**Usage**

Use this command to enable/disable CDR archival when a dead server is detected. With this CLI, once a server is detected as down, requests are purged. Also the requests generated for the period when the server is down are purged.
gtpp deadtime

Configures the amount of time to wait before attempting to communicate with a CGF that was previously marked as unreachable.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp deadtime <time>
```

* `time`  
  Default: 120  
  Specifies the amount of time that must elapse before the system attempts to communicate with a CGF that was previously unreachable.  
  `time` is measured in seconds and can be configured to any integer value from 1 to 65535.

Usage

If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down.  
This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.  
Refer to the `gtpp detect-dead-server` and `gtpp max-retries` commands for additional information on the process the system uses to mark a CGF as down.

Example

The following command configures the system to wait 60 seconds before attempting to re-communicate with a CGF that was marked as down:

```
gtpp deadtime 60
```
gtpp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a CGF as down.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp detect-dead-server consecutive-failures max_number
```

- `consecutive-failures max_number`:
  - Default: 0
  - Specifies the number of failures that could occur before marking a CGF as down.
  - `max_number` could be configured to any integer value from 0 to 1000.

Usage

This command works in conjunction with the `gtpp max-retries` parameter to set a limit to the number of communication failures that can occur with a configured CGF.

The `gtpp max-retries` parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The `gtpp detect-dead-server` parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicates with the CGF of next highest priority.

If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempts to communicate with the highest priority CGF again.

If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active.

Refer to the `gtpp max-retries` command for additional information.

Example

The following command configures the system to allow 8 consecutive communication failures with a CGF before it marks it as down:

```
gtpp detect-dead-server consecutive-failures 8
```


gtpp dictionary

This command designates specific dictionary used by GTPP for specific context.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom4 | custom5 | custom6 | custom7 | custom8 | custom9 | standard }
```

default gtpp dictionary

---

**default**

Configures the default dictionary.

---

**custom1**

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.

---

**custom2**

Custom-defined dictionary.

---

**custom3**

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 except that it supports the encoding of IP addresses in Binary format for G-CDRs.

---

**custom4**

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 except that:

- IP addresses are encoded in binary format
- the Data Record Format Version information element contains 0x1307 instead of 0x1308
- QoSRequested is not present in the LoTV containers
- QoSnegotiated is added only for the first container and the container after a QoS change

---

**custom5**

Custom-defined dictionary.

---

**custom6**

Custom-defined dictionary for eG-CDR encoding.
gtpp dictionary

**custom7 ... custom30**
Custom-defined dictionaries. These dictionary have default behavior or “standard” dictionary.

**standard**
Default: Enabled
A dictionary conforming to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

**Usage**
Use this command to designate specific dictionary used by GTPP for specific context.

**Example**
The following command configures the system to use custom3 dictionary to encode IP address in Binary format in G-CDRs:

```
gtpp dictionary custom3
```
**gtpp duplicate-hold-time**

This command configures the number of minutes to hold onto CDRs that are possibly duplicates while waiting for the primary CGF to come back up.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gtpp duplicate-hold-time minutes
```

*minutes*

Default: 60

When the primary CGF is down, the number of minutes to hold onto CDRs that may be duplicates. *minutes* must be an integer from 1 to 10080.

**Usage**

Use this command to configure how long to hold onto CDRs that are possibly duplicates while waiting for the primary CGF to come back up. If the GGSN determines that the primary CGF is down, CDRs that were sent to the primary CGF but not acknowledged are sent by the GSN to the secondary CGF as “possibly duplicates”. When the primary CGF comes back up, the GSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

**Example**

Use the following command to set the amount of time to hold onto CDRs to 2 hours (120 minutes);

```plaintext
gtpp duplicate-hold-time 120
```
gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp echo-interval *time*

no gtpp echo-interval

Example

The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new CGF server on the system using the *gtpp server* command as described in this chapter
- Upon the execution of the *gtpp test accounting* command as described in the Exec Mode Commands chapter of this reference
- Upon the execution of the *gtpp sequence-numbers private-extensions* command as described in this chapter

The echo-interval command is used in conjunction with the *gtpp max-retries* and *gtpp timeout* commands as described in this chapter.

In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.

The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the *gtpp deadtime* command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.
The following command configures an echo interval of 120 seconds:

```
gtpp echo-interval 120
```
**gtpp egcdr**

Configures the eG-CDR parameters and triggers.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
gtpp egcdr { final-record [ closing-cause [ same-in-all-partials | unique ] ] include-content-ids { all | only-with-traffic } [ closing-cause { same-in-all-partials | unique } ] | losdv-max-containers number | lotdv-max-containers number | service-data-flow threshold [ interval seconds ] | volume { downlink | total | uplink } | service-idle-timeout seconds }
```

```
default gtpp egcdr { final-record include-content-ids only-with-traffic closing-cause same-in-all-partials | losdv-max-containers | lotdv-max-containers | service-idle-timeout 0 }
```

```
no gtpp egcdr service-data-flow threshold [ interval | volume { downlink | uplink } | total | uplink [ downlink ] ]
```

| **final-record [ closing-cause [ same-in-all-partials | unique ] ] include-content-ids [ all | only-with-traffic ]** |
|---------------------------------------------------------------|
| Enables configuration of the final eG-CDR. |
| •**closing-cause** - Configures closing cause for the final eG-CDR. |
| •**same-in-all-partials** - Specifies that the same closing cause is to be included for multiple final eG-CDRs |
| •**unique** - Specifies that the closing cause for final eG-CDRs is to be unique. |
| •**include-content-ids** - Controls which content-ids are being included in the final eG-CDR. |
| •**all** - Specifies that all content-ids be included in the final eG-CDR. |
| •**only-with-traffic** - Specifies that only content-ids with traffic be included in the final eG-CDRs. |

<table>
<thead>
<tr>
<th><strong>losdv-max-containers number</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR. number can be configured to any integer value from 1 to 255.</td>
</tr>
<tr>
<td>Default: 10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>lotdv-max-containers number</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR. number can be configured to any integer value from 1 to 8.</td>
</tr>
<tr>
<td>Default: 8</td>
</tr>
</tbody>
</table>
Context Configuration Mode Commands

**service-data-flow threshold [ interval seconds | volume { downlink | total | uplink } bytes ]**

Configures the thresholds for closing a service data flow container within an eG-CDR.

- **interval** - configures the time interval in seconds
- **volume** - can specify uplink or downlink or combined total (uplink + downlink) byte thresholds.

A service data flow container has statistics for an individual content-id. When the threshold is reached, the service data flow container is closed.
Default: disabled

**service-idle-timeout seconds**

Specifies a time period where if no data is reported for a service flow, then the service container is closed and added to eG-CDR (as part of LOSDV container list) with service condition change as ServiceIdleOut.

*seconds* can be configured to any integer value from 10 to 86,400.
Default: 0. This means there is no service-idle-timeout trigger.

**Usage**

Use this command to configure individual triggers for eG-CDR generation.

**Example**

Use the following command to set the maximum number of LoSDV containers to 7.

```
gtp egcdr losdv-max-containers 7
```
**gtpp error-response**

This command configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp error-response { discard-cdr | retry-request }
```

```
default gtpp error-response
```

---

**default**
Resets the system’s configuration to the default value for error-response. Default is retry-request.

---

**discard-cdr**
Instructs the system to purge the request upon receipt of an error response and not to retry.

---

**retry-request**
Instructs the system to retry sending a DRT after receiving an error response. This is the default behavior.

---

**Usage**
This command configures the system’s response to receiving an error message after sending a DRT request.

---

**Example**

```
gtpp error-response discard-cdr
```
**gtpp group**

It configures GTPP server group in a context for the charging gateway function (CGF) accounting server(s) that the system is to communicate with.

**Product**

GGSN, SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
gtpp group group_name[-noconfirm]
```

*group_name*

Specifies the name of GTPP server group that is used for charging and/or accounting in a specific context.

*group_name* must be a string of size 1 to 63 character.

A maximum of 8 GTPP server groups (excluding system created default GTPP server group “default”) can be configured with this command in a context.

**no**

Removes the previously configured GTPP group within a context.

When a GTPP group is removed accounting information is not generated for all calls using that group and all calls associated with that group are dropped. A warning message displays indicating the number of calls that will be dropped.

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

This feature provides the charging gateway function (CGF) accounting server configurables for a group of servers. Instead of having a single list of CGF accounting servers per context, this feature configures multiple GTPP accounting server groups in a context and each server group is consist of list of CGF accounting servers.

In case no GTPP server group is configured in a context, a server group named “default” is available and all the CGF servers configured in a specific context for CGF accounting functionality will be part of this “default” server group.

**Example**

Following command configures a GTPP server group named *start* for charging gateway function accounting functionality and this server group is available for all subscribers with in that context.

```
gtpp group start
```
**gtpp max-cdtrs**

Configures the maximum number of charging data records (CDRs) included per packet.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp max-cdhrs number_cdhrs [ wait-time time ]
```

- **number_cdhrs**
  Default: 1
  Specifies the maximum number of CDRs to be inserted in a single packet.
  *number_cdhrs*: any integer value from 1 to 255.

- **wait-time time**
  Default: disabled
  Specifies the number of seconds the system waits for CDRs to be inserted into the packet before sending it.
  *time*: any integer from 1 to 300.

**Important:** If the *wait-time* expires, the packet is sent as this keyword over-rides *number_cdhrs*.

**Usage**

CDRs are placed into a GTPP packet as the CDRs close. The system stops placing CDRs into a packet when either the maximum *number_cdhrs* is met, or the *wait-time* expires, or the value for the *gtpp max-pdu-size* command is met.

**Example**

The following command configures the system to place a maximum of 10 CDRs in a single GTPP packet before transmitting the packet.

```
gtpp max-cdhrs 10
```
gtpp max-pdu-size

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp max-pdu-size

dfu_size

Default: 4096

Specifies the maximum payload size of the GTPP packet. The payload includes the CDR and the GTPP header.

Usage
The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and send the packet containing the one CDR regardless.

The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR.

The system performs standard IP fragmentation for packets that exceed the system’s maximum transmission unit (MTU).

Important: The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system’s max-pdu-size doesn't include the IPv4 and UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).

Example
The following command configures a maximum PDU size of 2048 octets:

    gtpp max-pdu-size 2048
gtpp max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive CGF.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
gtpp max-retries max_attempts
```

- `max_attempts`
  - Default: 4
  - Specifies the number of times the system attempts to communicate with a CGF that is not responding.
  - `max_attempts` can be configured to any integer value from 1 to 15.

**Usage**

This command works in conjunction with the `gtpp detect-dead-server` and `gtpp timeout` parameters to set a limit to the number of communication failures that can occur with a configured CGF. When the value specified by this parameter is met, a failure is logged. The `gtpp detect-dead-server` parameter specifies the number of consecutive failures that could occur before the server is marked as down. In addition, the `gtpp timeout` command controls the amount of time between re-tries. If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system’s memory buffer is exceeded. Refer to the `gtpp detect-dead-server` and `gtpp timeout` commands for additional information.

**Example**

The following command configures the maximum number of re-tries to be 8.

```bash
gtpp max-retries 8
```
gtpp node-id

This command configures the GTPP Node ID for all CDRs.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp node-id node_id

no gtpp node-id
```

```
no
Removes the previous gtpp node ID configuration.

node_id
Specifies the node ID for all CDRs.
node_id must be a string of 1 through 16 characters in length.
```

Usage
Use this command to configure the GTPP Node ID for all CDRs.

Example
The following command configures the GTPP Node ID as test123:

```
gtpp node-id test123
```
gtpp redirection-allowed

Configures the system to allow/disallow the redirection of CDRs when the primary CGF is unavailable.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp redirection-allowed

no gtpp redirection-allowed
```

Usage
This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the `no gtpp server` command. This functionality is enabled by default. If the `no gtpp redirection-allowed` command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, we will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.
gtpp redirection-disallowed

This command has been obsoleted and replaced with the `gtpp redirection-allowed` command.
gtpp server

Configures the charging gateway function (CGF) accounting server(s) that the system is to communicate with.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp server <ip_address> [ maxmsgs ] [ priority priority ] [ udp-port port ] [ node-alive { enable | disable } ] [-noconfirm ]

no gtpp server <ip_address>

no
Deletes a previously configured CGF.

<ip_address>
Specifies the IP address of the CGF in dotted decimal notation for IPv4 or colon notation for IPv6.

max msgs
Default: 256
Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets. msgs can be configured to any integer value from 1 to 256.

priority priority
Default: 1000
Specifies the relative priority of this CGF. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to. priority can be configured to any integer value from 1 to 1000. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the -noconfirm option, you are not asked for confirmation and multiple servers could be assigned the same priority.

udp-port port
Default: 3386
Specifies the UDP port over which the GSN communicates with the CGF. port can be configured to any integer value between 1 and 65535.

node-alive { enable | disable }
Default: Disable.
This optional keyword allows operator to enable/disable GSN to send Node Alive Request to GTPP Server (i.e. CGF). This configuration can be done per GTPP Server basis.
Context Configuration Mode Commands

-gtpserver

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to configure the CGF(s) that the system sends CDR accounting data to. Multiple CGFs can be configured using multiple instances of this command. Up to 12 CGFs can be configured per system context. Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of “1” has the highest priority.

Important: The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

Example

The following command configures a CGF with an IP address of 192.168.2.2 and a priority of 5.

    gtpserver 192.168.2.2 priority 5

The following command deletes a previously configured CGF with an IP address of 100.10.35.7:

    no gtpserver 100.10.35.7
**gtpp source-port-validation**

Toggles port checking for node alive/echo/redirection requests from the CGF.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
gtpp source-port-validation

[no | default] gtpp source-port-validation
```

- `no`
  
  Disables CGF port checking. Only the IP address will be used to verify CGF requests.

- `default`
  
  Restores this parameter to its default setting of enabled.

**Usage**

This command is for enabling or disabling port checking on node alive/echo/redirection requests from the CGF. If the CGF sends messages on a non-standard port, it may be necessary to disable port checking in order to receive CGF requests. On the default setting, both IP and port are checked.

**Example**

The following command disables port checking for CGF requests:

```plaintext
no gtpp source-port-validation
```
gtpp storage-server

Configures information for the GTPP back-up storage server.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp storage-server ip-address port port-num
no gtpp storage-server ip-address port port-num
```

no
Removes a previously configured back-up storage server.

ip-address
The IP address of the back-up storage server expressed in dotted decimal notation.

port port-num
Default: 3386
Specifies the UDP port number over which the GSN communicates with the back-up storage server.

Usage
This command configures the information for the server to which GTPP packets are to be backed-up to in the event that all CGFs are unreachable.
One backup storage server can be configured per system context.

Important: This command only takes affect if `gtpp single-source` in the Global Configuration Mode is also configured. Additionally, this command is customer specific. Please contact your local sales representative for additional information.

Example
The following command configures a back-up server with an IP address of 192.168.1.2:

```
gtpp storage-server 192.168.1.2
```
gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server. This command is available for ASR 5000 platform only.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```bash
gtpp storage-server local file { compression ( gzip | none ) | format ( custom1 | custom2 | custom3 | custom4 | custom5 | custom6 ) | name prefix | purge-processed-files [ purge-interval | purge_dur ] | rotation ( cdr-count | time-interval | volume | mbsize) }

default gtpp storage-server local file { compression | format | name prefix | purge-processed-files | rotation { cdr-count | time-interval | volume } }

no gtpp storage-server local file rotation { purge-processed-files | rotation { cdr-count | time-interval } }
```

no
Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.

compression ( gzip | none )
Configures the type of compression to be used on the files stored locally.
gzip — Enables Gzip file compression.
none — Disables Gzip file compression -this is the default value.

format ( custom-n )
Configures the file format to be used to format files to be stored locally.
custom1 — File format custom1 - this is the default value.
custom2 — File format custom2.
custom3 — File format custom3.
custom4 — File format custom4.
custom5 — File format custom5.
custom6 — File format custom6 with a block size of 8K for CDR files.

name prefix prefix
Defines the prefix to be used for the file name. By default the file name prefix would be ‘GTPP-group-name + VPN-ID’.
prefix — Enter a string of 1 to 64 alphanumeric characters.

purge-processed-files [ purge-interval purge_dur ]
Default: Disabled.
Enables the GSN to periodically (every 4 minutes) delete locally processed (*.p) CDR files from the HDD on the SMC card.

**Important:** This option is available only when GTPP server storage mode is configured for local storage of CDRs with the `gtpp storage-server mode local` command.

Optional keyword `purge-interval purge_dur` provides an option for user to control the purge interval duration in minutes by setting `purge_dur`. `purge_dur` must be an integer between 1 through 259200. Which has a default value of 60 minutes.

```
rotation { cdr-count count | time-interval time | volume mb size }
```

Specifies rotation related configuration for GTPP files stored locally.
- `cdr-count count`—Configure the CDR count for the file rotation. Enter a value from 1000 to 65000. Default value 10000.
- `time-interval time`—Configure the time interval for file rotation. Enter a value in seconds ranging from 30 to 86400. Default value is 3600 seconds (1 hour).
- `volume mb size`—Configure the file volume, in MB, for file rotation. Enter a value ranging from 2 to 40. This trigger can not be disabled. Default value is 10MB.

**Usage**

This command configures the parameters for storage of GTPP packets as files on the local server - meaning the hard disk.

**Example**

The following command configures rotation for every 1.5 hours for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400
```
**gtpp storage-server max-retries**

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp storage-server max-retries max_attempts
```

`max_attempts`
Default: 2
Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding.

`max_attempts` can be configured to any integer value from 1 to 15.

**Usage**
This command works in conjunction with the `gtpp storage-server timeout` parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server.
The `gtpp storage-server timeout` command controls the amount of time between re-tries.
Refer to the `gtpp storage-server timeout` command for additional information.

**Example**
The following command configures the maximum number of re-tries to be 8.

```
gtpp storage-server max-retries 8
```
gtpp storage-server mode

This command configures storage mode, local or remote, for CDRs. Local storage mode is available with ASR 5000 platforms only.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp storage-server mode { local | remote | streaming }

default gtpp storage-server mode

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Returns the GTPP group configuration to the default 'remote' value for the GTPP storage server mode.</td>
</tr>
<tr>
<td>local</td>
<td>Default: Disabled. Specifies the use of the hard disk on the SMC for storing CDRs</td>
</tr>
<tr>
<td>remote</td>
<td>Specifies the use of an external server for storing CDRs. This is the default value.</td>
</tr>
<tr>
<td>streaming</td>
<td>Default: Disabled. This keyword allows the operator to configure &quot;streaming&quot; mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:</td>
</tr>
</tbody>
</table>

  - When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.
  - If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF. |

Usage
This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.

Example
The following command configures use of a hard disk for storing CDRs.

```
   gtpp storage-server mode local
```
gtpp storage-server timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp storage-server timeout duration
```

*duration*
Default: 30

Specifies the maximum amount of time the system waits for a response from the GTPP back-up storage server before assuming the packet is lost.

*duration* is measured in seconds and can be configured to any integer value from 30 to 120.

Usage

This command works in conjunction with the `gtpp storage-server max-retries` command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of 60 seconds:

```
gtpp storage-server timeout 60
```
gtpp suppress-cdrs zero-volume-and-duration

This command suppresses the CDRs created by session having zero duration and/or zero volume. By default this mode is ‘disabled’.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp suppress-cdrs zero-volume-and-duration { gcdrs [egcdrs] | egcdrs [gcdrs] }  
default gtpp suppress-cdrs zero-volume-and-duration
```

**default**
Disables the CDR suppression mode.

**gcdrs [egcdrs]**
Specifies that this command will handle G-CDRs before eG-CDRs.

**egcdrs [gcdrs]**
Specifies that this command will handle eG-CDRs before G-CDRs.

Usage
Use this command to suppress the CDRs (G-CDRs and eG-CDRs) which were created due with zero-duration session and zero-volume session due to any reason. By default this command is disabled and system will not suppress any CDR.

Example
The following command configures the system to suppression the eG-CDRs created for a zero duration session or zero volume session:

```
gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs
```
gtpp timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the CGF.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp timeout time
```

Default: 20
Specifies the maximum amount of time the system waits for a response from the CGF before assuming the packet is lost.
`time` is measured in seconds and can be configured to any integer value from 1 to 60.

Usage
This command works in conjunction with the `gtpp max-retries` command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged. This parameter specifies the time between retries.

Example
The following command configures a retry timeout of 30 seconds:

```
gtpp timeout 30
```
gtpp trigger

This command is left in place for backward compatibility. To disable and enable GTPP triggers you should use the `gtpp trigger` command in GTPP Server Group Configuration mode.
**gtpp transport-layer**

This command selects the transport layer protocol for Ga interface for communication between AGW (GSNs) and GTPP servers.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp transport-layer { tcp | udp }
```

```
default gtpp transport-layer
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Resets the transport layer protocol to GTPP servers to the default UDP.</td>
</tr>
</tbody>
</table>
| **tcp** | Default: Disabled
Enables the system to implement TCP as transport layer protocol for communication with GTPP server. |
| **udp** | Default: Enabled
Enables the system to implement UDP as transport layer protocol for communication with GTPP server. |

**Usage**
Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

**Example**
The following command enables TCP as the transport layer protocol for the GSN’s Ga interface.

```
gtpp transport-layer tcp
```
gtpu-service

Creates a GTP-U service or specifies an existing GTP-U service and enters the GTP-U service configuration mode for the current context.

Product
GGSN, P-GW, S-GW

Privilege
Administrator

Syntax

```
gtpu-service service_name [ -noconfirm ]
no gtpu-service service_name
```

*service_name*

Specifies the name of the GTP-U service. If *service_name* does not refer to an existing service, a new service is created if resources allow.

*service_name* must be from 1 to 63 alpha and/or numeric characters.

* -noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

```
no gtpu-service service_name
```

Removes the specified GTP-U service from the context.

Usage

Enter the GTP-U service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

⚠️ Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-gtpu-service)#
```

GTP-U Service Configuration Mode commands are defined in the GTP-U Service Configuration Mode Commands chapter.

Example

The following command enters the existing GTP-U service configuration mode (or creates it if it doesn’t already exist) for the service named *gtpu-service1*:
The following command will remove `gtpu-service1` from the system:

```
no gtpu-service gtpu-service1
```
ha-service

Creates/deletes a home agent service or specifies an existing HA service for which to enter the home agent service configuration mode for the current context.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ha-service name
no ha-service name
```

- **name**
  Specifies the name of the HA service to configure. If `name` does not refer to an existing service, the new service is created if resources allow. `name` must be from 1 to 63 alpha and/or numeric characters.

**Usage**
Enter the HA service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

**Example**
The following command will enter the HA service configuration mode creating the service `sampleService`, if necessary.

```
ha-service sampleService
```

The following command will remove `sampleService` as being a defined HA service.

```
no ha-service sampleService
```
**hnbgw-service**

This command creates/removes an Home NodeB Gateway (HNB-GW) service or configures an existing HNB-GW service and enters the HNB-GW service configuration mode for Femto UMTS access networks in the current context.

**Product**
HNB-GW

**Privilege**
Administrator

**Syntax**

```
hnbgw-service service_name [-noconfirm]
no hnbwg-service service_name
```

**no**
Removes the specified HNB-GW service from the context.

```
service_name
```

Specifies the name of the HNB-GW service. If `service_name` does not refer to an existing service, the new service is created if resources allow.

*service_name* must be from 1 to 63 alpha and/or numeric characters.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to enter the HNB-GW service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 8 HNB-GW service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

⚠️ **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hnbgw-service)#
```

The commands configured in this mode are defined in the *HNB-GW Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

⚠️ **Caution:** This is a critical configuration. The HNB-GW service can not be configured without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration will stop the HNB-GW service.
Example
The following command enters the existing HNB-GW service configuration mode (or creates it if it doesn’t already exist) for the service named `hnb-service1`:

```
hnbgw-service hnb-service1
```

The following command will remove `hnb-service1` from the system:

```
no hnbgw-service hnb-service1
```
hsgw-service

Creates an HSGW service or specifies an existing HSGW service and enters the HSGW service configuration mode for the current context.

Product
HSGW

Privilege
Administrator

Syntax

hsgw-service service_name [ -noconfirm ]

no hsgw-service service_name

service_name
Specifies the name of the HSGW service. If service_name does not refer to an existing service, the new service is created if resources allow.

- noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Enter the HSGW service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

[context_name]hostname(config-hsgw-service)#

HSGW Service Configuration Mode commands are defined in the HSGW Service Configuration Mode Commands chapter.

Use this command when configuring the following eHRPD components: HSGW.

Example
The following command enters the existing HSGW service configuration mode (or creates it if it doesn’t already exist) for the service named hsgw-service1:
The following command will remove `hsgw-service1` from the system:

```
no hsgw-service hsgw-service1
```
ikev1 disable-phase1-rekey

This command configures the rekeying of Phase1 SA when the Internet Security Association and Key Management Protocol (ISAKMP) lifetime expires in Internet Key Exchange (IKE) v1 protocol.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] ikev1 disable-phase1-rekey

no
Disable this command which re-enables Phase 1 SAs when the ISAKMP lifetime expires.

Usage
Use this command to disable the rekeying of Phase 1 SAs when the ISAKMP lifetime expires in IKE v1 protocol.

Example
The following command disables rekeying of Phase1 SAs when the lifetime expires:

    ikev1 disable-phase1-rekey
ikeyv1 keepalive dpd

This command configures the ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] ikeyv1 keepalive dpd interval interval timeout timeout num-retry retries
```

- **no**
Deletes previously configured IPSec DPD Protocol settings.

- **interval interval**
The time interval at which IPSec DPD Protocol messages are sent.
  - `interval` is measured in seconds and can be configured to any integer value between 10 and 3600.

- **timeout time**
The amount of time allowed for receiving a response from the peer security gateway prior to re-sending the message.
  - `time` is measured in seconds and can be configured to any integer value between 10 and 3600.

- **num-retry retries**
The maximum number of times that the system should attempt to reach the peer security gateway prior to considering it unreachable.
  - `retries` can be configured to any integer value between 1 and 100.

**Usage**

Use this command to configure the ISAKMP dead peer detection parameters in IKE v1 protocol.

Tunnels belonging to crypto groups are perpetually kept “up” through the use of the IPSec Dead Peer Detection (DPD) packets exchanged with the peer security gateway.

**Important:** The peer security gateway must support RFC 3706 in order for this functionality to function properly.

This functionality is for use with the Redundant IPSec Tunnel Fail-over feature and to prevent IPSec tunnel state mismatches between the FA and HA when used in conjunction with Mobile IP applications. Regardless of the application, DPD must be supported/configured on both security peers. If the system is configured with DPD but it is communicating with a peer that does not have DPD configured, IPSec tunnels still come up. However, the only indication that the remote peer does not support DPD exists in the output of the `show crypto isakmp security associations summary dpd` command.
\textbf{Important:} If DPD is enabled while IPSec tunnels are up, it will not take affect until all of the tunnels are cleared.

**Example**
The following command configures IPSec DPD Protocol parameters to have an interval of 15, a timeout of 10, to retry each attempt 5 times:

```
ikev1 keepalive dpd interval 15 timeout 10 num-retry 5
```
ikev1 policy

This command configures/creates an ISAKMP policy with the specified priority and enters ISAKMP Configuration Mode for IKE v1 protocol.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] ikev1policy priority

no
Removes a previously configured ISAKMP policy for IKE v1 protocol.

priority
Default: 0
This must be an integer from 0 through 100. ISAKMP policies for IKE v1 protocol with lower priority numbers take precedence over policies with higher priorities. “0” is the highest priority.

Usage
Use this command to create ISAKMP policies to regulate how IPSec key negotiation is performed for IKE v1 protocol.
Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (i.e. which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.
During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKE SAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.
Multiple ISAKMP policies can be configured in the same context and are used in an order determined by their priority number.

Example
Use the following command to create an ISAKMP policy with the priority 1 and enter the ISAKMP Configuration Mode:
ikev1 policy 1
ikev2-ikesa

Creates a new, or specifies an existing, IKEv2 security association transform set and enters the IKEv2 Security Association Configuration Mode.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

[ no ] ikev2-ikesa transform-set name

name
Specifies the name of a new or existing security association transform set. name must be from 1 to 127 alpha and/or numeric characters.

Usage
Use this command to create a new or enter an existing IKEv2 security association transform-set. A list of up to four separate transform-sets can be created.
Entering this command results in the following prompt:
[context_name]hostname(cfg-ctx-ikev2ikesa-tran-set)#
IKEv2 Security Association Configuration Mode commands are defined in the IKEv2 Security Association Configuration Mode Commands chapter.

Example
The following command configures an IKEv2 security association transform set called ikesa3 and enters the IKEv2 Security Association Configuration Mode:

ikev2-ikesa transform-set ikesa3
ims-auth-service

This command creates the specified IMS authorization service, and enters the IMS Authorization Service Configuration Mode within the current context for Gx/Ty interface support to a subscriber session for IMS authorization and flow-based charging procedures.

Product
PDSN, GGSN, HA

Privilege
Security Administrator, Administrator

Syntax

ims-auth-service auth_svc_name [ -noconfirm ]

[ no | default ] ims-auth-service auth_svc_name

---

**no**
Deletes the specified IMS authorization service with in specific context.

---

**default**
Restores default state of IMS authorization service, disabled for specific context.

---

**auth_svc_name**
Specifies the unique name of IMS authorization service across the system to be configured for Gx/Ty interface authentication within specific context.

*auth_svc_name* must be a unique string of 1 through 63 characters in length.

A maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.

---

**-noconfirm**
Specifies that the command is to execute without any additional prompt and confirmation from the user.

---

Usage
Use this command to create/delete an IMS authorization service for Gx/Ty interface for a subscriber.

---

Example
The following command configures an IMS authorization service *ims_interface1* with in this context:

```
ims-auth-service ims_interface1
```
**ims-sh-service**

This command creates the specified IMS Sh service name to allow configuration of Sh service.

**Product**
PDIF, SCM

**Privilege**
Administrator

**Syntax**

```plaintext
ims-sh-service name
no ims-sh-service name
```

**Usage**

Removes a previously configured IMS-Sh-service.

```plaintext
name
```

Name of the IMS-Sh-service to be configured. *name* must be from 1 to 63 alpha and/or numeric characters.

**Example**
The following example names a service to be configured:

```plaintext
ims-sh-service ims-1
```
inspector

Configures a context-level inspector account within the current context.

**Product**

All

**Privilege**

Security Administrator

**Syntax**

```
inspector user_name [ encrypted ] password pwd [ ecs | noecs ] [ expiry-date date_time ] [ li-administration ] [ noecs ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [ timeout-idle idle_seconds ] [ timeout-min-idle idle_minutes ]
```

**no inspector user_name**

- **no**
  
  Removes a previously configured inspector account.

- **user_name**
  
  Specifies a name for the context-level inspector account. user_name must be from 1 to 32 alpha and/or numeric characters.

- **[ encrypted ] password pwd**
  
  Specifies the password to use for the user which is being given context-level inspector privileges within the current context. The encrypted keyword indicates the password specified uses encryption.
  
  The password specified as pwd must be from 1 to 63 alpha and/or numeric characters without encryption and must be from 1 to 127 alpha and/or numeric characters when encryption has been indicated.
  
  The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

- **[ ecs | noecs**
  
  Default: *noecs*
  
  ecs - Permits the specific user to access ACS-specific configuration commands.
  
  noecs - Prevents the specific user to access ACS-specific configuration commands.

- **expiry-date date_time**
  
  The date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.
  
  Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.
li-administration
Permits this user to execute Lawful Intercept commands.

Important: Users who have Lawful Intercept privileges are only given those privileges when connected to the system through a Secure Shell (SSH). If this user connects through a Telnet session or through the console port, Lawful Intercept privileges are not enabled.

timeout-absolute abs_seconds
Default: 0
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of time, in seconds, the context-level inspector may have a session active before the session is forcibly terminated. abs_seconds must be a value in the range from 0 through 300000000.
The special value 0 disables the absolute timeout.

timeout-min-absolute abs_minutes
Default: 0
Specifies the maximum amount of time, in minutes, the context-level inspector may have a session active before the session is forcibly terminated. abs_minutes must be a value in the range from 0 through 525600 (365 days).
The special value 0 disables the absolute timeout.

timeout-idle idle_seconds
Default: 0
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of idle time, in seconds, the context-level inspector may have a session active before the session is terminated. idle_seconds must be a value in the range from 0 through 300000000.
The special value 0 disables the idle timeout.

timeout-min-idle idle_minutes
Default: 0
Specifies the maximum amount of idle time, in minutes, the context-level inspector may have a session active before the session is terminated. idle_minutes must be a value in the range from 0 through 525600 (365 days).
The special value 0 disables the idle timeout.

Usage
Create new context-level inspector or modify existing inspector’s options, in particular, the timeout values.
Inspector users have minimal read-only privileges. Refer to the Command Line Interface Overview chapter of Cisco ASR 5000 Series Command Line Interface Reference for more information.

Important: A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example
The following command creates a context-level inspector account named user1:

    inspector user1 password secretPassword

The following command removes a context-level inspector account named user1:

    no inspector user1
interface

Creates/deletes an interface or specifies an existing interface. By identifying an interface, the mode changes to configure this interface in the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

interface name [ broadcast | loopback | point-to-point | tunnel ]

do interface name

no
Indicates the interface specified is to be removed.

name
Specifies the name of the interface to configure. If name does not refer to an existing interface, the new interface is created if resources allow. name must be from 1 to 79 alpha and/or numeric characters.

broadcast
Default: Enabled
Creates an Ethernet broadcast (IP) interface and enters the Ethernet configuration mode.

Important: Refer to the Ethernet interface Configuration Mode Command chapter for more information.

loopback
Default: Disabled
Creates an internal IP address that can be reached by any interface configured in the current context. The interface must be configured for loopback when configuring Interchassis Session Recovery. A total of 256 loopback interfaces can be configured.

Important: Refer to the Loopback Interface Configuration Mode Command chapter for more information.

point-to-point
 Creates a permanent virtual connection (PVC) in the current context and enters the PVC configuration mode. Currently, this type of interface is only used with an optical (ATM) line card.

Important: Refer to the PVC interface Configuration Mode Command chapter for more information.
tunnel

Creates a tunnel interface to support the various tunnel interfaces. Currently only IPv6-over-IPv4 and GRE tunnel interface is supported.

**Important:** Refer to the Tunnel Interface Configuration Mode Command chapter for more information.

Usage

Use this command to enter/create the interface configuration mode for an existing interface or for a newly defined interface. This command is also used to remove an existing interface when it longer is needed.

**Important:** If no keyword is specified, broadcast is assumed and the interface is Ethernet by default.

For IPv6-over-IPv4 or GRE tunneling user need to specify the interface type as `tunnel`.

Example

The following command enters the Ethernet Interface Configuration mode creating the interface `sampleService`, if necessary.

```
interface sampleInterface
```

The following command removes `sampleService` as being a defined interface.

```
no interface sampleInterface
```

The following command enters the Tunnel Interface Configuration mode creating the interface `GRE_tunnel1`, if necessary.

```
interface GRE_tunnel1 tunnel
```
ip

The commands in this section set context level IP parameters.
ip access-group

Configures access group with access control list (ACL) for IP traffic for the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

    ip access-group name [ in | out ] [ priority_value ]
    no ip access-group name [ in | out ]

    no
    Indicates the specified ACL rule is to be removed from the group.

    name
    Specifies the ACL rule to be added/removed from the group.
    In Release 8.1 and later, name must be an alpha and/or numeric string of 1 through 47 characters in length.
    In Release 8.0, name must be an alpha and/or numeric string of 1 through 79 characters in length.

**Important:** Up to 8 ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 256 rule limit for the context.

    in | out
    The in and out keywords are deprecated and are only present for backward compatibility. The Context-level ACL are applied only to outgoing packets.

    priority_value
    Default: 0
    Specifies the priority of the access group. 0 is the highest priority. If priority_value is not specified, the priority is set to 0. priority_value must be an integer from 0 through 4294967295.
    If access groups in the list have the same priority, the last one entered is used first.

Usage

Use this command to add IP access lists (refer to the ip access-list command) configured with in the same context to an ACL group.
Refer to the Access Control Lists chapter of the System Enhanced Feature Configuration Guide for more information ACLs and ACL rules.

Example

The following commands add sampleGroup to the context-level ACL with a priority of 0.
ip access-group sampleGroup 0
ip access-list

This command enables creating/configuring/deleting an IP Access List in the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ip access-list <name>
[ default | no ] ip access-list <name>

default
Sets the context’s default access control list to that specified by <name>.

no
Removes the specified access list.

name
Specifies the access list name.
In Release 8.0, <name> must be an alpha and/or numeric string of 1 through 79 characters in length.
In Release 8.1 and later, <name> must be an alpha and/or numeric string of 1 through 47 characters in length.
If the named access list does not exist, it is created, and the CLI mode changes to the Access Control List Configuration Mode, wherein the access list can be configured.
If the named access list already exists, the CLI mode changes to the Access Control List Configuration mode, wherein the access list can be reconfigured.

Usage
Executing this command enters the Access Control List Configuration Mode in which rules and criteria are defined for the ACL.

**Important:** A maximum of 64 rules can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it's typically less than 200.

The no version of this command deletes the ACL.
Refer to the Configuring and Applying Access Control Lists chapter of the System Administration Guide for more information on ACLs and ACL rules.

Example
The following command creates an access list named `sampleList`, and enters the Access List configuration mode:

`ip access-list sampleList`
ip access-list
ip arp

Configures the address resolution protocol options for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip arp ip_address mac_address[vrf vrf_name]

no ip arp ip_address

no

Indicates the ARP configuration data for the IP address specified is to be removed from the configuration.

ip_address

Specifies the IP address to configure the ARP options where ip_address must be specified using the standard IPv4 dotted decimal notation.

mac_address

Specifies the media-specific access control layer address for the IP address. mac_address must be specified as a an 6-byte hexadecimal number with each byte separated by a colon, e.g., ‘AA:12:bb:34:f5:0E’.

vrf vrf_name

This keyword associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry. vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context configuration mode through ip vrf command.

Usage

Manage the IP address mapping which is a logical/virtual identifier to the more lower layer addressing used for address resolution in ICMP messages.

For tunnel-based interface, network IP pool can have overlapping ip-addresses across VRFs. To manage it adding a preconfigured VRF context is required to associate with an static ARP entry. By default, the ARP is added in the given context. If the VRF name is specified, then the ARP is added to the VRF ARP table.

Example

The following commands set the IP and MAC address for the current context then remove it from the configuration.

    ip arp 1.2.3.4 F1:E2:D4:C5:B6:A7

    no ip arp 1.2.3.4

The following commands set the IP and MAC address for a VRF context GRE_vrf1 in the configuration.

    ip arp 1.2.3.4 F1:E2:D4:C5:B6:A7 vrf GRE_vrf1
ip arp
ip as-path access-list

Defines BGP AS Path access lists.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

ip as-path access-list list_name{deny | permit}reg_expr
no ip as-path access-list list_name{deny | permit}reg_expr

no
Remove the specified regular expression from the AS path access list.

list_name
To add new rules to an existing list, enter the list name. list_name must be a string of alpha numerical characters from 1 through 79 characters.

{deny | permit}
deny: Deny access to AS paths that match the regular expression.
permit: Allow access to AS paths that match the regular expression.

reg_expr
A regular expression to define the AS paths to match. reg_expr must be a string containing 1 through 254 alpha and/or numeric characters.

Important: The ? (question mark) character is not supported in regular expressions for this command.

Usage
Use this command to define AS path access lists for the BGP router in the current context. The chassis supports a maximum of 64 access lists per context.

Example
The following command creates an AS access list named ASlist1 and permits access to AS paths.

ip as-path access-list ASlist1 permit
ip dns-proxy source-address

Enables the proxy DNS functionality and identifies this context as the destination context for all redirected DNS requests.

**Important:** This command must be entered in the destination context for the subscriber. If there are multiple destination contexts for different subscribers, the command must be entered in each context.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**


```plaintext
[ no ] ip dns-proxy source-address ip_address
```

- **no**
  
  Removes the address in this context as a destination for redirected DNS packets.

- **ip dns-proxy source-address ip_address**
  
  Specifies an interface in this context used for redirected DNS packets. `ip_address` must be specified using the standard IPv4 dotted decimal notation.

**Usage**

Use this command to identify the interface in this context where redirected DNS packets are sent to the home DNS. The system uses this address as the source address of the DNS packets when forwarding the intercepted DNS request to the home DNS server. For a more detailed explanation of the proxy DNS intercept feature, see the `proxy-dns intercept-list` command.

**Example**

The following command identifies an interface with an address of 1.23.456.456 in a destination context where the system forwards all intercepted DNS requests:

```plaintext
ip dns-proxy source-address 1.23.456.456
```
ip domain-lookup

Enables/disables domain name lookup via domain name servers for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip domain-lookup</td>
</tr>
<tr>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>

- **no**
  Disables domain name lookup.

**Usage**
Domain name lookup is necessary if the subscribers configured for the context are to be allowed to use logical host names for services which requires the host name resolution via DNS.

**Example**

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip domain-lookup</td>
</tr>
<tr>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>
**ip domain-name**

Configures/removes the logical domain name for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip domain-name name
no ip domain-name name
```

`no`
Indicates the logical domain name for the current context is to be removed.

`name`
Specifies the logical domain name to use for domain name server address resolution. `name` must be from 1 to 1023 alpha and/or numeric characters formatted to be a valid IP domain name.

**Usage**
Set a logical domain name if the context is to be accessed by logical domain name in addition to direct IP address.

**Example**

```
ip domain-name sampleName.org
```
ip forward

This command configures an IP forwarding policy to forward outgoing pool packets whose flow lookup fails to the default-gateway.

By default the behavior is to either send an ICMP Unreachable message or to discard the packet depending on the configuration of the IP pool.

Pool packets coming from the linecard whose flow lookup fails are discarded or ICMP unreachable is sent irrespective of whether the above command is configured or not.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[no] ip forward outbound unused-pool-dest-address default-gateway

no
Disable forwarding to the default gateway.

Usage
Use this command to set an IP forwarding policy that forwards outgoing pool packets whose flow lookup fails to the default-gateway.

Example
To enable this functionality, enter the following command:

    ip forward outbound unused-pool-dest-address default-gateway

To disable this functionality, enter the following command:

    no ip forward outbound unused-pool-dest-address default-gateway
ip identification packet-size-threshold

Configures the packet size above which system will assign unique IP header identification.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

ip identification packet-size-threshold size

default ip identification packet-size-threshold

default
Restores default value of 576 bytes to IP packet size for fragmentation threshold.

size
Default: 576 bytes.
Specifies the size of IP packet in bytes above which system will assign unique IP header identification for system generated IP encapsulation headers. (such as MIP data tunnel).
size can be configured to any integer value from 0 to 2000.

Usage
This configuration is used to set the upper limit of the IP packet size. All packets above that size limit will be considered ‘fragmentable’, and an unique non-zero identifier will be assigned.

Example
The following commands set the IP packet size to 1024 bytes as threshold. above this limit system will assign unique IP header identification for system generated IP encapsulation headers:

ip identification packet-size-threshold 1024
ip localhost

Configures or removes the static local host logical name to IP address mapping for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip localhost name ip_address
no ip localhost name ip_address
```

<table>
<thead>
<tr>
<th>no</th>
<th>Indicates the static mapping is to be removed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the logical host name for the local machine the current context resides on. <em>name</em> must be from 1 to 1023 alpha and/or numeric characters formatted to be a valid IP host name.</td>
</tr>
<tr>
<td>ip_address</td>
<td>Specifies the IP address for the static mapping. <em>ip_address</em> must be specified using the standard IPv4 dotted decimal notation.</td>
</tr>
</tbody>
</table>

**Usage**
Avoid excessive DNS lookups across the network by statically mapping the logical host name to the local host’s context.

**Example**

```
ip localhost localhostName 1.2.3.4
no ip localhost localhostName 1.2.3.4
```
ip name-servers

Modifies the list of domain name servers the current context may use for logical host name resolution.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip name-servers ip_address secondary_ip_address
no ip name-servers ip_address
```

**no**
Indicates the name server specified is to be removed from the list of name servers for the current context.

**ip_address**
Specifies the IP address of a domain name server. *ip_address* must be specified using the standard IPv4 dotted decimal notation.

**secondary_ip_address**
Specifies the IP address of a secondary domain name server. *secondary_ip_address* must be specified using the standard IPv4 dotted decimal notation.

Usage
Manage the list of name servers the current context may use in resolving logical host names.
The DNS can be specified at the Context level in Context configuration as well as at the APN level in APN configuration mode with **dns** and **ipv6 dns** commands, or it can be received from AAA server.
When DNS is requested in PCO configuration, the following preference will be followed for DNS value:
1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN with **dns** and **ipv6 dns** commands has the third preference.
4. DNS values configured at context level has the last preference.

**Important:** The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

Example

```
ip name-servers 1.2.3.4
```
ip pool

This command enables to add/configure/delete IP address pools in the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip pool pool_name { ip_address subnet_mask | ip_address_mask_combo | range start_ip_address end_ip_address } [ address_hold_timer address_hold_timer ] [ advertise-if-used ] [ alert-threshold { group-available | pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] ] [ explicit-route-advertise ] [ group-name group_name ] [ include-nw-bcast ] [ napt-users-per-ip-address users_per_ip ] [ alert-threshold { { pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] } + ] [ max-chunks-per-user max_chunks_per_user [ nat-binding-timer nat_binding_timer ] [ next-hop-forwarding-address ip_address ] [ on-demand ] [ port-chunk-size port_chunk_size ] [ port-chunk-threshold port_chunk_threshold ] [ send-nat-binding-update ] + ] [ nat_priority ] [ nat-one-to-one [ alert-threshold { { pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] } + ] [ nat-binding-timer nat_binding_timer ] [ next-hop-forwarding-address ip_address ] [ on-demand ] [ send-nat-binding-update ] + ] [ nat-realm users-per-nat-ip-address users [ on-demand [ address_hold_timer address_hold_timer ] ] ] [ next-hop-forwarding-address ip_address [ overlap_vlanid vlan_id ] [ respond-icmp-echo ip_address ] ] [ nw-reachability server server_name ] [ policy allow-static-allocation ] [ private_priority ] [ public_priority ] [ resource_priority ] [ send-icmp-dest-unreachable ] [ srp-activate ] [ static ] [ suppress-switchover-arps ] [ tag { none | pdif-setup-addr } ] [ unicast-gratuitous-arp-address ip_address ] [ vrf vrf_name { [ mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ] } ] +

no ip pool pool_name [ address_hold_timer ] [ advertise-if-used ] [ alert-threshold { { group-available | pool-free | pool-hold | pool-release | pool-used } + ] [ explicit-route-advertise ] [ group-name ] [ include-nw-bcast ] [ next-hop-forwarding-address [ respond-icmp-echo ] ] [ nw-reachability server ] [ policy allow-static-allocation ] [ send-icmp-dest-unreachable ] [ srp-activate ] [ suppress-switchover-arps ] [ tag { none | pdif-setup-addr } ] [ unicast-gratuitous-arp-address ] + [ send-nat-binding-update ]

no

Removes the specified IP address pool from the current context’s configuration, or disables the specified option(s) for the specified IP pool.

no alert-threshold

This command without any optional keywords disables all alert thresholds.
name

Specifies the logical name of the IP address pool. name must be an alpha and/or numeric string of 1 through 31 characters in length.

Important: An error message displays if the ip pool name and the group name in the configuration are the same. An error message displays if the ip pool name or group name are already used in the context.

ip_address

Specifies the beginning IP address of the IP address pool. ip_address can either be an IPv4 address expressed in dotted decimal notation, or an IPv6 address expressed in colon notation.

subnet_mask

Specifies the IP address mask bits to determine the number of IP addresses in the pool. ip_mask must be specified using the standard IPv4 dotted decimal notation.

1 bits in the ip_mask indicate that bit position in the ip_address must also have a value of 1.

0 bits in the ip_mask indicate that bit position in the ip_address does not need to match, i.e., the bit can be either a 0 or a 1.

For example, if the IP address and mask are specified as 172.168.10.0 and 255.255.255.224, respectively, the pool will contain IP addresses in the range 172.168.10.0 through 172.168.10.31 for a total of 32 addresses.

ip_address_mask_combo

Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. ip_address_mask_combo must be specified using the form ‘IP Address/Mask Bits’ where the IP address is specified using the standard IPv4 dotted decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

range start_ip_address end_ip_address

Specifies the IP addresses for the IP pool as a range of addresses.

start_ip_address specifies the beginning of the range of addresses for the IP pool.

end_ip_address specifies the end of the range of addresses for the IP pool.

The IP address range must be specified using the standard IPv4 dotted decimal notation.

For example, if start_ip_address is specified as 172.168.10.0 and end_ip_address is specified as 172.168.10.31 the IP pool will contain addresses in the range 172.168.10.0 through 172.168.10.31 for a total of 32 addresses.

private [ priority ]

Address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. priority must be a value in the range from 0 through 10 with 0 being the highest priority. The default value is 0.

public [ priority ]

Address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. priority must be a value in the range from 0 through 10 with 0 being the highest priority. The default value is 0.
**static**
Address pool is used for statically assigned mobile stations. Statically assigned mobile stations are those with a fixed IP address at all times.

**tag { none | pdif-setup-addr }**
Default: none
none: default tag for all IP address pools
pdif-setup-addr: pool with this tag should only be used for PDIF calls.

**address-hold-timer seconds**
When this is enabled, and an active subscriber is disconnected, the IP address is held, or considered still in use, and is not returned to the free state until the address-hold-timer expires. This enables subscribers who reconnect within the length of time specified (in seconds) to obtain the same IP address from the IP pool. 
seconds is the time in seconds and must be an integer from 0 through 31556926.

**alert-threshold { group-available | pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ]**
Default: All thresholds are disabled.
Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IP pool thresholds.
group-available: Set an alert based on the available percentage of IP addresses for the entire IP pool group.
pool-free: Set an alert based on the percentage of IP addresses that are unassigned in this IP pool.
pool-hold: Set an alert based on the percentage of IP addresses from this IP pool that are on hold.
pool-release: Set an alert based on the percentage of IP addresses from this IP pool that are in the release state.
pool-used: This command sets an alert based on the percentage of IP addresses that have been assigned from this IP pool.

**Important:** Refer to the threshold available-ip-pool-group and threshold monitoring commands in this chapter for additional information on IP pool utilization thresholding.

low_thresh: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100.
clear high_thresh: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. It may be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**group-name group_name**
Assigns preconfigured one or more IP pools to the IP pool group group_name. group_name is case sensitive and must be a string of 1 to 31 characters. One or more IP pool groups are assigned to a context and one IP pool group consists one or more IP pool(s).
IP pool group name is used in place of an IP pool name. When specifying a desired pool group in a configuration the IP pool with the highest precedence is used first. When that IP pool’s addresses are exhausted the pool with the next highest precedence is used.

**include-nw-bcast**

Includes the network and broadcast addresses as part of the pool. To remove the include-nw-bcast option from the ip pool, use the `no ip pool test include-nw-bcast` command.

```
napt-users-per-ip-address users_per_ip [ alert-threshold { ( pool-free | poolhold | pool-release | pool-used ) low_thres [ clear high_thres ] } + ] [ max-chunks-per-user max_chunks_per_user [ nat-binding-timer nat_binding_timer ] [ next-hop-forwarding-address ip_address ] [ on-demand ] [ port-chunk-size port_chunk_size ] [ port-chunk-threshold port_chunk_threshold ] [ send-nat-binding-update ] +
```

**Important:** In UMTS deployments this keyword is available in Release 9.0 and later releases. In CDMA deployments this keyword is available in Release 8.3 and later releases.

**Important:** In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to 8.3, all NAT realms configured in Release 8.1 using the `nat-one-to-one` keyword must be reconfigured using either the `nat-one-to-one` (for one-to-one NAT realms) or the `napt-users-per-ip-address` (for many-to-one NAT realms) keywords.

Configures many-to-one NAT realms.
- **users_per_ip:** Specifies how many users can share a single NAT IP address. `users_per_ip` must be an integer from 2 through 2016.
- **alert-threshold:** Specifies alert threshold for the pool:

```
<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool-free</td>
<td>Percentage free alert threshold for this pool</td>
</tr>
<tr>
<td>pool-hold</td>
<td>Percentage hold alert threshold for this pool</td>
</tr>
<tr>
<td>pool-release</td>
<td>Percentage released alert threshold for this pool</td>
</tr>
<tr>
<td>pool-used</td>
<td>Percentage used alert threshold for this pool</td>
</tr>
<tr>
<td>low_thres</td>
<td>The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. <code>low_thres</code> must be an integer from 0 through 100.</td>
</tr>
<tr>
<td>clear high_thres</td>
<td>The IP pool utilization percentage that maintains a previously generated alert condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. <code>high_thres</code> must be an integer from 0 through 100.</td>
</tr>
</tbody>
</table>
```

**Important:** Thresholds configured using the `alert-threshold` keyword are specific to the pool that they are configured in. Thresholds configured using the `threshold ip-pool-*` commands in the Context Configuration Mode apply to all IP pools in that context, and override the threshold configurations set within individual pools.
Context Configuration Mode Commands

**ip pool**

### Important:
The `high_thresh` value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

- **max-chunks-per-user**
  - **max_chunks_per_user**: Specifies the maximum number of port chunks to be allocated per subscriber in the many-to-one NAT pool. `max_chunks_per_user` must be an integer from 1 through 2016. Default: 1

- **nat-binding-timer**
  - **binding_timer**: Specifies NAT Binding Timer for the NAT pool. `timer` must be an integer from 0 through 31556926. If set to 0, is disabled. Default: 0

- **nexthop-forwarding-address**
  - **address**: Specifies the nexthop forwarding address for this pool. `address` must be a standard IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

### Important:
The `nexthop-forwarding-address` support for NAT IP pools is functional only in later releases of Release 9.0 and in Release 10.0 and later releases.

- **on-demand**: Specifies allocating IP when matching data traffic begins.

- **port-chunk-size**
  - **size**: Specifies NAT port chunk size (number of NAT ports per chunk) for many-to-one NAT pool. `size` must be an integer from 32 through 32256.

### Important:
The `port-chunk-size` configuration is only available for many-to-one NAT pools.

- **port-chunk-threshold**
  - **chunk_threshold**: Specifies NAT port chunk threshold in percentage of number of chunks for many-to-one NAT pool. `chunk_threshold` must be an integer from 1 through 100. Default: 100%

### Important:
The `port-chunk-threshold` configuration is only available for many-to-one NAT pools.

- **send-nat-binding-update**
  - **Default**: Disabled

### Important:
`send-nat-binding-update` is not supported for many-to-one realms.

The following IP pool configuration keywords can also be used in the many-to-one NAT pool configuration:

- **group-name**
  - **group_name**: This keyword is available for NAT pool configuration only in Release 10.0 and later releases.
    - Specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group.
    - NAT pool and NAT pool group names must be unique.
    - `group_name` must be an alpha and/or numeric string of 1 through 31 characters in length, and is case sensitive.

- **srp-activate**
nat priority

Designates the IP address pool as a Network Address Translation (NAT) address pool.

priority specifies the priority of the NAT pool. 0 is the highest priority. If priority is not specified, the priority is set to 0.

Must be a value from 0 (default) to 10.

**Important:** This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

```
nat-one-to-one [ alert-threshold { ( pool-free | pool-hold | pool-release | pool-used ) low_thresh [ clear high_thresh ] } + ] [ nat-binding-timer nat_binding_timer ] [ nexthop-forwarding-address ip_address ] [ on-demand ] [ send-nat-binding-update ] +
```

**Important:** In UMTS deployments this keyword is available in Release 9.0 and later releases. In CDMA deployments this keyword is available in Release 8.3 and later releases.

**Important:** In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to Release 8.3, all NAT realms configured in Release 8.1 using the nat-realm keyword must be reconfigured using either the nat-one-to-one (for one-to-one NAT realms) or the napt-users-per-ip-address (for many-to-one NAT realms) keywords.

Configures one-to-one NAT realm.

• **alert-threshold**: Specifies alert threshold for this pool:

**Important:** Thresholds configured using the alert-threshold keyword are specific to the pool that they are configured in. Thresholds configured using the threshold ip-pool *commands in the Context Configuration Mode apply to all IP pools in the context, and override the threshold configurations set within individual pools.

• **pool-free**: Percentage free alert threshold for this pool
• **pool-hold**: Percentage hold alert threshold for this pool
• **pool-release**: Percentage released alert threshold for this pool
• **pool-used**: Percentage used alert threshold for this pool
• **low_thresh**: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. low_thresh must be an integer from 0 through 100.
• **clear high_thresh**: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. high_thresh must be an integer from 0 through 100.

**Important:** The high_thresh value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.
**nat-binding-timer** *nat_binding_timer*: Specifies NAT binding timer for the NAT pool. *binding_timer* must be an integer from 0 through 31556926. If set to 0, is disabled.

**Important:** For many-to-one NAT pools, the default NAT binding timer value is 60 seconds. For one-to-one NAT pools, it is 0. I.e., by default, the feature is disabled—the IP addresses/ port-chunks once allocated will never be freed.

**nexthop-forwarding-address** *ip_address*: Specifies the nexthop forwarding address for this pool. *address* must be a standard IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

**Important:** The **nexthop-forwarding-address** support for NAT IP pools is functional only in later releases of Release 9.0 and in Release 10.0 and later releases.

**on-demand**: Specifies allocating IP address when matching data traffic begins.

**send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

**Important:** **send-nat-binding-update** is not supported for many-to-one realms.

The following IP pool configuration keywords can also be used in the one-to-one NAT pool configurations:

- **address-hold-timer** *address_hold_timer*
- **group-name** *group_name*: This keyword is available for NAT pool configuration only in Release 10.0 and later releases.
  - Specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group.
  - NAT pool and NAT pool group names must be unique.
  - *group_name* must be an alpha and/or numeric string of 1 through 31 characters in length, and is case sensitive.

**srp-activate**

```plaintext	nat-realm users-per-nat-ip-address users [ on-demand [ address-hold-timer address_hold_timer ] ]
```

**Important:** The **nat-realm** keyword is only available in Release 8.1.

**Important:** In Release 8.1, the NAT On-demand feature is not supported.

**Important:** This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

Designates the IP address pool as a Network Address Translation (NAT) realm pool.

- **users-per-nat-ip-address** *users*: Specifies the number of users sharing a single NAT IP address. *users* must be an integer from 1 through 5000.
- **on-demand**: Specifies to allocate IP when matching data traffic begins.
**address-hold-timer** *address_hold_timer*: Specifies the address hold timer for this pool, in seconds. *address_hold_timer* must be an integer from 0 through 31556926. If set to 0, the address hold timer is disabled.

**nexthop-forwarding-address** *ip_address*

A subscriber that is assigned an IP address from this pool is forwarded to the next hop gateway with the specified IP address.

**overlap vlanid** *vlan_id*

When a nexthop forwarding address is configured, this keyword can be configured to enable over-lapping IP address pool support and associates the pool with the specified virtual LAN (VLAN).

For more information on configuring VLANs, refer to the *System Enhanced Features Guide*. *vlan_id* is the identification number of a VLAN assigned to a physical port and can be configured to any integer value from 1 to 4095.

**Important**: This functionality is currently supported for use with systems configured as an HA, or as a PDSN for Simple IP, or as a GGSN. This keyword can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 256 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per HA or simple IP PDSN. For GGSNs, the total number of pools is limited by the number of VLANs defined but the maximum number per context is 256. Additional network considerations and configuration outside of the system may be required.

**nw-reachability server** *server_name*

Bind the name of a configured network reachability server to the IP pool and enable network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration.

*server_name*: Specifies the name of a network reachable server that has been defined in the current context, and must be a string of 1 through 16 characters in length.

**Important**: Also see the following commands for more information: Refer to the *policy nw-reachability-fail* command in the HA Configuration Mode to configure the action that should be taken when network reachability fails. Refer to the *nw-reachability-server* command in this chapter to configure network reachability servers. Refer to the *nw-reachability-server* command in the Subscriber Configuration Mode to bind a network reachability server to a specific subscriber.

**respond-icmp-echo** *ip_address*

Pings the first IP address from overlapping IP address pools.

**Important**: In order for this functionality to work, all of the pools should contain an initial IP address that can be pinged.

**resource**

Default: Disabled

Specifies this IP pool as a resource pool. The IP addresses in resource pools may have IP addresses that exist in other resource pools. IP addresses from a resource pool should not be used for IP connectivity within the system where the pool is defined. These IP addresses should be allocated for sessions which are L3 tunneled...
through the system (IP-in-IP or GRE). It is possible for resource pools in the same context to have overlapping addresses when the terminating network elements for the L3 tunnels are in different VPNs. Also refer to the subscriber configuration mode `13-to-12-tunnel address-policy` command.

**send-icmp-dest-unreachable**
Default: Disabled
When enabled, this generates an ICMP destination unreachable PDU when the system receives a PDU destined for an unused address within the pool.

**explicit-route-advertise**
Default: Enabled
When enabled, the show ip pool verbose output includes the total number of explicit host routes.

**srp-activate**
Activates the IP pool for Interchassis Session Redundancy.

**suppress-switchover-arp**
Default: Disabled
Suppress corresponding gratuitous ARP generation when a line card switchover occurs.

**unicast-gratuitous-arp-address** `ip_address`
Default: Perform broadcast gratuitous ARP.
Perform a unicast gratuitous ARP to the specified IP address rather than broadcast gratuitous ARP when gratuitous ARP generation is required.

```plaintext
vrf vrf_name { [ mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ] ] }
```
This keyword associates a preconfigured Virtual Routing and Forwarding (VRF) context instance with this IP pool and configures the other MPLS label parameters like values of In and Out labels.

**Important:** This command must be used with next-hop parameters.

- `vrf_name` is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context configuration mode through `ip vrf` command.
  - `in_label_value` is the MPLS label that identifies the inbound traffic destined for this pool.
  - The `out_label_value1` and `out_label_value2` identify the MPLS labels to be added to the outgoing packets sent for subscriber from this pool. Where `out_label_value1` is the inner output label and `out_label_value2` is the outer output label.

MPLS label values must be an integer from 16 to 1048575.
By default, the pools configured are bound to the default VRF unless specified with a VRF name.

**Important:** You cannot have overlapping pool addresses using the same VRF. Also you cannot have two pools using different VRF’s but the same in-label irrespective of whether the pools are overlapping or not. The pool must be private or static pool in-order to be associated with a certain VRF. If the VRF with such a name is not configured, then the pool configuration would return an error prompting to add the VRF before configuring a pool.
**policy allow-static-allocation**

Configures static address allocation policy for dynamic IP pool. This keyword enables a dynamic IP pool to accept a static address for allocation.

---

**Important:** In static allocation scenario, the pool group name is returned by AAA in the attribute SN1-IP-Pool-Name, and the IP address to use will be returned in the Framed-IP-Address attribute.

---

Indicates that more than one of the previous keywords can be entered within a single command.

---

**Usage**

Define one or more pools of IP addresses for the context to use in assigning IPs to mobile stations. This command is also useful in resizing existing IP pools to expand or contract the number of addresses allocated. If you resize an IP pool, the change is effective immediately. When using the ip pool command to resize an IP pool, the type must be specified since by default the command assumes the type as public. In other words, the CLI syntax to resize an ip pool is the same syntax used to create the pool. See examples below.

```
ip pool pool1 100.1.1.0/24 static
```

Then the syntax to resize that pool would be

```
ip pool pool1 100.1.1.0/25 static
```

A pool which is deleted will be marked as such. No new IP addresses will be assigned from a deleted pool. Once all assigned IP addresses from a deleted pool have been released, the pool, and all associated resources, are freed.

---

**Important:** If an IP address pool is matched to a ISAKMP crypto map and is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the `clear crypto` command in the Exec mode for information on clearing security associations.

---

**Over-lapping IP Pools** - The system supports the configuration of over-lapping IP address pools within a particular context. Over-lapping pools are configured using either the resource or overlap keywords. The `resource` keyword allows over-lapping addresses tunneled to different VPN end points. The `overlap` keyword allows over-lapping addresses each associated with a specific virtual LAN (VLAN) configured for an egress port. It uses the VLAN ID and the nexthop address to determine how to forward subscriber traffic with addresses from the pool thus resolving any conflicts with over-lapping addresses. Note that if an overlapping IP Pool is bound to an IPSec Tunnel (refer to the `match ip pool` command in the Crypto Group Configuration Mode chapter), that tunnel carries the traffic ignoring the nexthop configuration. Therefore, the IPSec Tunnel takes precedence over the nexthop configuration. (Thus, one can configure the overlapping IP Pool with fake VLAN ID and nexthop and still be able to bind it to an IPSec Tunnel for successful operation.

The `overlap` keyword allows over-lapping addresses each associated with a specific VLAN can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 128 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per system.
**Important:** Overlapping IP address functionality is currently supported for use with systems configured as an HA for Mobile IP, or as a PDSN for Simple IP, or as a GGSN. For deployments in which subscriber traffic is tunneled from the FA to the HA using IP-in-IP, a separate HA service must be configured for each overlapping pool.

**IP Pool Address Assignment Method** - IP addresses can be dynamically assigned from a single pool or from a group of pools. The addresses are placed into a queue in each pool. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

**Important:** Note that setting different priorities on each individual pool in a group can cause addresses in some pools to be used more frequently.

**Example**
The following commands define a private IP address pool, a public IP address pool and a static address pool, respectively.

```
ip pool samplePool1 1.2.3.0 255.255.255.0 private
ip pool samplePool2 1.3.0.0 255.255.0.0 public 1
ip pool samplePool3 1.4.5.0 255.255.255.0 static
```

The following command defines a private IP pool specified with a range of IP addresses. The pool has 101 addresses.

```
ip pool samplePool4 range 1.5.5.0 1.5.5.100 private
```

The following command sets the address hold timer on the pool to 60 minutes (3600 seconds):

```
ip pool samplePool4 address-hold-timer 3600
```

The following command removes the IP address pool from the configuration:

```
no ip pool samplePool1
```

The following command creates a static IP pool:

```
ip pool pool1 100.1.1.0/24 static
```

The following command resizes the static IP pool created in the previous example:

```
ip pool pool1 100.1.1.0/25 static
```
ip prefix-list

Creates an IP prefix list for filtering routes.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
ip_prefix-list name list_name [ seq seq_number ] { deny | permit } { any | network_address/net_mask [ ge ge_value ] [ le le_value ]

no
Delete the specified prefix-list entry.

name list_name
Specifies a name for the prefix list. list_name must be a string of 1 through 79 characters in length.

seq seq_number
Assign the specified sequence number to the prefix list entry. seq_number must be an integer from 1 through 4294967295.

deny
Specify prefixes to deny.

permit
Specify prefixes to permit.

any
Match any prefix.

network_address/net_mask [ ge ge_value ] [ le le_value ]
The prefix to match.

ge ge_value: The minimum prefix length to match. This must be an integer from 0 through 32. If only the ge value is specified, the range is from the ge value to 32. The ge value must be greater than net_mask and less than the le value.

le le_value: The maximum prefix length to match. This must be an integer from 0 through 32. If only the le value is specified, the range is from the net_mask to the le value. The le value must be less than or equal to 32.
```
The following equation describes the conditions that ge and le values must satisfy:

\[ \text{net\_mask} \leq \text{ge\_value} \leq \text{le\_value} \leq 32 \]

**Usage**

Use this command to filter routes by their IP prefix.

**Example**

```
ip prefix-list name prelist10 seq 5 permit 192.168.100.0/8 ge 12 le 24
```
ip prefix-list sequence-number

This enables and disables the inclusion of IP prefix list sequence numbers in the configuration file. This is enabled by default.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

ip prefix-list sequence-number
no ip prefix-list sequence-number

Usage
Use this command to enable and disable the inclusion of IP prefix list sequence numbers in the configuration file.

Example
To disable the inclusion of IP prefix list sequence numbers in the configuration file, enter the following command:

no ip prefix-list sequence-number
ip route

Adds/removes routing information from the current context’s configuration.

**Product**

All

**Privilege**

Administrator

**Syntax**

```
[ no ] ip route {ip_address/ip_mask | ip_address ip_mask} { gateway_ip_address |
next-hop next_hop_ip_address | point-to-point | tunnel} egress_intrfc_name [
cost cost ] [ precedence precedence ] [ vrf vrf_name ]
```

**no**

Indicates the route specified by this option is to be removed from the configuration.

```
ip_address/ip_mask | ip_address ip_mask
```

Specifies a destination IP address or group of addresses that will use this route.

- **ip_address/ip_mask**: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ip_address/ip_mask* must be specified using the form ‘IP Address/Mask Bits’ where the IP address is specified using the standard IPv4 dotted decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

- **ip_address ip_mask**: Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. *ip_address/ip_mask* must be specified using the standard IPv4 dotted decimal notation. *ip_mask* must be specified using the standard IPv4 dotted decimal notation as network mask for subnets.

The mask as specified by *ip_mask* or resulting from *ip_address/ip_mask* is used to determine the network for packet routing.

0’s in the resulting mask indicate the corresponding bit in the IP address is not significant in determining the network for packet routing.

1’s in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network.

```
gateway_ip_address | next-hop next_hop_ip_address | point-to-point |
tunnel
```

Specifies which device or network to use when forwarding packets.

- **gateway_ip_address**: Specifies the IP address of the network gateway to which to forward packets. The address must be entered in IPv4 dotted decimal notation (###.###.###.###).

- **next-hop next_hop_ip_address**: The next-hop IP address to which to forward packets. The address must be entered in IPv4 dotted decimal notation (###.###.###.###).

- **point-to-point**: Specifies that the egress port is an ATM point-to-point interface.

- **tunnel**: This keyword sets the static route for this egress interface as tunnel type. i.e. IPv6-over-IPv4 or GRE.
**Context Configuration Mode Commands**

- **ip route**

### Context Configuration Mode Commands

- **egress_intrfc_name**
  
  Specifies the name of the egress (out-bound) interface name in the current context. The `egress_intrfc_name` must be from 1 to 79 alpha and/or numeric characters.

- **cost cost**
  
  Default: 0
  
  Specifies the relative cost of the route. The `cost` must be a value in the range 0 through 255, where 255 is the most expensive.

- **precedence precedence**
  
  Default: 1
  
  Specifies the selection order precedence for this routing information. The `precedence` must be a value in the range from 1 through 254, where 1 is the highest precedence.

- **vrf vrf_name**
  
  This keyword associates a Virtual Routing and Forwarding (VRF) context with this static route configuration. The `vrf_name` is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context configuration mode through the `ip vrf` command.

### Usage

Use this command to configure the IP route parameters. Precedence and cost options are used to tailor the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route’s being selected first by lower precedence then the cost is used if multiple route’s are defined with the same precedence.

**Important:** A maximum of 1200 static routes may be configured per context.

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for GRE tunneling support.

### Example

The following command adds a route using the combined IP address and subnet mask form:

```
ip route 1.2.3.0/32 192.168.1.2 egressSample1 precedence 160
```

The following configures route options for a route specified using the distinct IP address and subnet mask form:

```
ip route 1.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following deletes the two routes configured above:

```
no ip route 1.2.3.0/32 192.168.1.2 egressSample1 precedence 160
no ip route 1.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following command adds a route using the combined IP address and subnet mask form and specifies the egress interface as tunnel type:

```
ip route 1.2.3.0/32 tunnel egressSample1 precedence 160 vrf GRE_vrf1
```
Context Configuration Mode Commands

ip route
ip routing maximum-paths

This command enables Equal Cost Multiple Path (ECMP) routing support and specifies the maximum number of ECMP paths that can be submitted by a routing protocol in the current context.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
ip routing maximum-paths [max_no]
[ default | no ] ip routing maximum-paths
```

**default**
Resets the command to its default setting of 4.

**no**
Disables ECMP for the current context.

**max_no**
Default: 4
The maximum number of ECMP paths that can be submitted by a routing protocol. max_no must be an integer from 1 through 10.

Usage
Use this command to enable ECMP for routing and set the maximum number of ECMP paths that can be submitted by a routing protocol.

Example
To enable ECMP and set the maximum number of paths that may be submitted by a routing protocol in the current context to 10, enter the following command:

```
   ip routing maximum-paths 10
```

To disable ECMP in the current context, enter the following command:

```
   no ip routing maximum-paths
```
ip routing overlap-pool

Configures the routing behavior for overlap-pool addresses.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | default ] ip routing overlap-pool
```

- **default**
  Resets the command to it’s default setting of disabled.

- **no**
  Disables the routing behavior for overlap-pool addresses for the current context.

**Usage**

Default: disabled

Use this command configuration to advertise overlap-pool addresses in dynamic routing protocols when overlap pools are configured using vlan-ids. If the “ip routing overlap-pool” is configured, then the overlap-addresses are added as interface addresses and advertised.
**ip vrf**

This command creates a Virtual Routing and Forwarding (VRF) context instance, assigns a VTF id, and configures the VRF parameters for BGP MPLS VPN and GRE tunnel interface configuration.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip vrf vrf_name
no ip vrf
```

**no**

Disables IP Virtual Routing and Forwarding (VRF) parameters.

**vrf_name**

Specifies the name of the virtual routing and forwarding interface. `vrf_name` must be an alpha and/or numeric string of 1 to 79 characters.

**Usage**

Use this command to create a VRF context and assigns a VRF id to this instance. This command used when system works as a BGP router with MPLS VPN and binds a MPLS VPN to system or to facilitate GRE tunnelling. The addresses that assigned to this interface are visible in the VRF routing table.

This command switches the command mode to *IP VRF Context Configuration Mode* and prompt will be changed to the following:

```
[context_name>]host_name(config-context-vrf)#
```

If required, this command creates IP Virtual Routing and Forwarding context configuration mode instance. While using this command user must take note of the following:

- A VRF context instance must be created and configured before referring, associating, or binding the same with any command or mode.
- If interface binding to a VRF context instance is changed or any IP address assigned to the interface is deleted a warning will be displayed.
- All interface bind with a VRF context instance will be deleted when that VRF is removed/deleted.
- An interface can be bound to only one VRF context instance.
- A maximum of 100 VRF context instances can be configured on a systme.

Kindly refer *IP VRF Context Configuration Mode Commands* chapter for parameter configurations.

**Example**
Following command configures the virtual routing and forwarding context instance $GRE_vrf1$ in a context:

```
ip vrf GRE_vrf1
```
ipms

Enables/disables/manages an intelligent packet monitoring system (IPMS) client service and enters the IPMS client configuration mode within the current context.

**Important:** The IPMS is a license enabled external application support. Refer to the IPMS Installation and Administration Guide for more information on this product.

**Product**
IPMS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ipms[-noconfirm ]
```

- **no**
  Deletes a previously configured IPMs client service.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Warning:** If this keyword option is used with `no ipms` command the IPMS client service will be deleted with all active/inactive IPMS sessions without prompting any warning or confirmation.

**Usage**
Use this command to enable/disable/manage the IPMS client service within a context and configure certain functionality. This command enables and allows the configuration of service enabling the system to function as an IPMS-enabled Access Gateway in a network. This command is also used to remove previously configured IPMS client service. A maximum of 1 IPMS client can be configured per system. Refer to the IPMS Installation and Administration Guide and IPMS Configuration Mode chapter of this reference for additional information.

**Example**
The following command creates an IPMS client service name within the context:

```
ipms
```
ipsec

Creates a new, or specifies an existing, IPSec transform set and enters the IPSec Transform Set Configuration Mode for the current context.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

[ no ] ipsec transform-set name


name
Specifies the name of a new or existing transform set. name must be from 1 to 127 alpha and/or numeric characters.

Usage
Use this command to create an new or enter an existing IPSec transform-set. Up to four transform-sets can be created.
Entering this command results in the following prompt:
[context_name]hostname(cfg-ctx-ipsec-tran-set)#

IPSec Transform Set Configuration Mode commands are defined in the IPSec Transform Set Configuration Mode Commands chapter.

Example
The following command configures an IPSec transform set called ipsec12 and enters the IPSec Transform Set Configuration Mode:

ipsec transform-set ipsec12
ipsg-service

Creates an IP Services Gateway service, or specifies an existing IPSG service, in the current context and enters the IPSG RADIUS Snoop or IPSG RADIUS Server Configuration Mode.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

```
ipsg-service name [ mode { radius-server | radius-snoop } ] [ -noconfirm ]
no ipsg-service name [ mode { radius-server | radius-snoop } ]
```

no

Removes the IPSG service from the system.

name

Specifies the name of the IPSG service to be configured. If name does not refer to an existing service, the new service is created if resources allow. name must be an alpha and/or numeric string of 1 through 63 characters in length.

mode { radius-server | radius-snoop }

Configures the IPSG to perform as either a RADIUS server or as a device to extract user information from RADIUS accounting request messages (snoop). If the mode optional keyword is not entered, the system defaults to radius-server.

radius-server: Creates an IP Services Gateway RADIUS Server service in the context and enters the IPSG RADIUS Server Configuration Mode.

radius-snoop: Creates an IP Services Gateway RADIUS Snoop service in the context and enters the IPSG RADIUS Snoop Configuration Mode.

-noconfirm

Indicates that the command is to execute without an additional prompt and confirmation from the user.

Usage

Enter the IPSG RADIUS Snoop or IPSG RADIUS Server Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of one IPSG service can be configured per context.

Entering this command results in the following prompt (RADIUS Server shown):  
```
[context-name-service-name]hostname(config-radius-server)#
```

IPSG service commands are defined in the IPSG RADIUS Snoop Configuration Mode Commands chapter or the IPSG RADIUS Server Configuration Mode Commands chapter of the Cisco ASR 5000 Series Command Line Interface Reference.

A maximum of 256 services (regardless of type) can be configured per system.
Caution: A large number of services greatly increases the complexity of system management and may impact overall system performance (i.e., resulting from system handoffs). Do not configure a large number of services unless your application requires it. Contact your local service representative for more information.

Important: IP Services Gateway functionality is a license-controlled feature. A valid feature license must be installed prior to configuring an IPSG service. If you have not previously purchased this feature, contact your sales representative for more information.

For more information about the IP Services Gateway, refer to the IP Services Gateway Configuration Guide.

Example
The following command configures an IPSG RADIUS Snoop service named ipsg1 and enters the IPSG RADIUS Snoop Configuration Mode:

```
ipsg-service ipsg1 mode radius-snoop
```
**ipv6 access-group**

Configures the IPv6 Access group.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ipv6 access-group group name \{ priority_value \}
```

- **group_name**
  Specifies the name of the access group. group_name must be an alpha and/or numeric string of 1 to 79 characters.

- **priority_value**
  Default: 0
  Specifies the priority of the access group. 0 is the highest priority. If **priority_value** is not specified the priority is set to 0. **priority_value** must be a value from 0 to 4294967295. If access groups in the list have the same priority, the last one entered is used first.

**Usage**

Use this command to specify Ipv6 access group name and priority. Use a lower value to indicate a higher priority for the group.

**Example**

```
ipv6 access-group group_1
```
**ipv6 access-list**

Configures access list (or packet filter) name and enters the IPv6 access list configuration mode.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ipv6 access-list name
```

- **no**
  Indicates the access list specified is to be removed from the configuration.

- **name**
  Specifies the access list for which to enter the access list configuration mode or the list to remove. `name` must be from 1 to 79 alpha and/or numeric characters.

**Usage**

Executing this command enters the Access Control List Configuration Mode in which rules and criteria are defined for the ACL.

**Example**

```
ipv6 access-list samplelist
no ipv6 access-list samplelist
```
ipv6 dns-proxy

Configures the domain name server proxy for the context.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

ipv6 dns-proxy source-ipv4-address ip_address

no ipv6 dns-proxy source-ipv4-address ip_address

no
Removes the predefined IP address for local interface in the destination context.

source-ipv4-address
Enables the IPv6 proxy DNs functionality for a context. It makes PDSN to use this address as the source address of the IPv4 packets.
Default: no address is configured.

ip_address
Specifies the IPv4 address of one of the local interface in the destination context to configure the IPv6 DNS proxy where ip_address must be specified using the standard IPv4 dotted decimal notation.

Usage
The IPv6 DNS proxy source IPv4 address is used as the source IP address for the DNS proxy transaction.

Example
The following command provides an example of configuring a IPv6 DNS proxy of 192.168.23.1:

ipv6 dns-proxy source-ipv4-address 192.168.23.1
ipv6 neighbor

Add a static IPv6 neighbor entry into the neighbor discovery table.

Product
PDIF

Privilege
Administrator, Security Administrator

Syntax

\[
\text{[ no ] ipv6 neighbor ipv6_address hardware_address}
\]

- no
  Removes the specified address.

\[
\text{ipv6 neighbor ipv6_address hardware_address}
\]

ipv6_address is the IP address of node to be added to the table.
hardware_address is the associated 48-bit MAC address.

Usage
Add a static IPv6 neighbor entry into the neighbor discovery table.

Example
Add the ipv6 address \text{fe80::210:83ff:ef7:7a9d::/24} and associated 48 bit MAC address \text{0:10:83:f7:7a:9d} to the table.

\[
\text{ipv6 neighbor fe80::210:83ff:ef7:7a9d::/24 0:10:83:f7:7a:9d}
\]
**ipv6 pool**

Modifies the current context’s IP address pools by adding, updating, or deleting a pool. Also use this command to resize an existing IP pool.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ipv6 pool name{ 6to4 local-endpoint ipv4_address[ default-relay-router_address] | alert threshold | group-name name | policy { allow-static-allocation | dup-addr-detection | prefix ipv4_address | default-relay-router_address | range start_address end_address | suppress-switchover-arps } [ private_priority] | [ public_priority] | [ shared_priority] | [ static_priority] | [ group-name name]

no ipv6 pool name
```

- **no**
  Deletes the previously configured ipv6 pool.

- **name**
  Specifies the logical name of the IP address pool. *name* must be from 1 to 31 alpha and/or numeric characters.

- **6to4-tunnel local-endpoint ip_address**
  Specifies the IPv4 Address of the local interface to be used for 6to4 compatible pool address construction.

- **alert threshold**
  Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IPv6 pool thresholds.
  - **6to4** - Sets an alert based on the IPv6 Pool for 6to4 compatible address type.
  - **alert-threshold** - Sets an alert based on the percentage free alert threshold for this group.
  - **group-available** - Sets an alert based on the percentage free alert threshold for this group.
  - **group-name** - Sets an alert based on the IPv6 Pool Group.
  - **policy allow-static-allocation** - Sets an alert based on the address allocation policy.
  - **pool-free** - Sets an alert based on the percentage free alert threshold for this pool.
  - **pool-used** - Sets an alert based on the percentage used alert threshold for this pool.
**ipv6 pool**

- **prefix** - Sets an alert based on the IPv6 Pool address prefix.
- **range** - Sets an alert based on the IPv6 address pool range of addresses.
- **suppress-switchover-arps** - Sets an alert based on the Suppress Gratuitous ARPS when performing a line card switchover.

```plaintext
context Configuration Mode Commands

ipv6 pool

- prefix - Sets an alert based on the IPv6 Pool address prefix.
- range - Sets an alert based on the IPv6 address pool range of addresses.
- suppress-switchover-arps - Sets an alert based on the Suppress Gratuitous ARPS when performing a line card switchover.

---

group name name
IPv6 Pool Group.
The following options are available:
- 6to4 - IPv6 Pool for 6to4 compatible address type
- alert-threshold - Percentage free alert threshold for this group
- group-name - IPv6 Pool Group
- policy - Configure an address allocation policy
- prefix - IPv6 Pool address prefix
- range - Configures IPv6 address pool to use a range of addresses
- suppress-switchover-arps - Suppress Gratuitous ARPS when performing a line card switchover

---

ipv4_address
Specifies the beginning IPv4 address of the IPv4 address pool. `ipv4_address` must be specified using the standard IPv4 dotted decimal notation.

---

default-relay-router router address
Specifies the default relay router for the tunnel.

---

policy allow-static-allocation
Allows a dynamic pool to accept a static address allocation.
The following options are available:
- 6to4 - IPv6 Pool for 6to4 compatible address type
- alert-threshold - Percentage free alert threshold for this group
- group-name - IPv6 Pool Group
- policy - Configure an address allocation policy
- prefix - IPv6 Pool address prefix
- range - Configures IPv6 address pool to use a range of addresses
- suppress-switchover-arps - Suppress Gratuitous ARPS when performing a line card switchover

---

policy dup-addr-detection
Default: Disabled.
This command is valid for IPv6 shared pools only (Sample syntax: `ipv6 pool name prefix ip_address/len shared policy dup-addr-detection`). When this policy is enabled, the IPv6 shared pool allows a prefix to be shared in different call sessions with different interface IDs for an IPv6 address. This allows the tracking of interface IDs per prefix and the detection of duplicated IDs.
With this policy disabled, the IPv6 shared pool will allow a prefix to be shared across different call sessions. The interface ID is not considered for any duplicate address detection.
The following options are available:
Context Configuration Mode Commands

ipv6 pool

- 6to4 - IPv6 pool for 6to4 compatible address type
- alert-threshold - Percentage free alert threshold for this group
- group-name - IPv6 pool group
- policy - Configure an address allocation policy
- prefix - IPv6 pool address prefix
- range - Configures IPv6 address pool to use a range of addresses
- suppress-switchover-arps - Suppress gratuitous ARPS when performing a line card switchover

prefix ip_address/len
Specifies the beginning IPv6 address of the IPv6 address pool. ip_address/len must be specified using colon notation.

range start_address end_address
Configures IPv6 address pool to use a range of addresses.
start_address specifies the beginning of the range of addresses for the IPv6 pool.
end_address specifies the end of the range of addresses for the IPv6 pool.

suppress-switchover-arps
Suppresses Gratuitous ARPS when performing a line card switchover.
The following options are available:
- 6to4 - IPv6 Pool for 6to4 compatible address type
- alert-threshold - Percentage free alert threshold for this group
- group-name - IPv6 Pool Group
- policy - Configure an address allocation policy
- prefix - IPv6 Pool address prefix
- range - Configures IPv6 address pool to use a range of addresses
- suppress-switchover-arps - Suppress Gratuitous ARPS when performing a line card switchover

private priority | public priority | shared priority | static priority
Default: public
private priority: address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. priority must be a value in the range from 0 through 10 with 0 being the highest. The default is 0.
public priority: address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. priority must be a value in the range from 0 through 10 with 0 being the highest and with a default of 0.
shared priority: address pool that may be used by more than one session at any time. priority must be a value in the range from 0 through 10 with 0 being the highest and with a default of 0.
static priority: address pool is used for statically assigned mobile stations. Statically assigned mobile stations are those with a fixed IP address at all times. priority must be a value in the range from 0 through 10 with 0 being the highest and with a default of 0.
This keyword is used to group the IPv6 pools in to different groups. The subscribers/domain can be configured with the group-name instead of the prefix-pool names.

`name` is the name of the group by which the IPv6 pool is to be configured and must be a string having 1 to 79 alpha and/or numeric characters.

**Usage**

Use this command to modify the current context’s IP address pools by adding, updating, or deleting a pool. Also use this command to resize an existing IP pool.

**Example**

Following command provides an example of adding IPv6 pool named `ip6Star`.

```
ipv6 pool ip6Star
```
ipv6 route

Configures a static IPv6 route to the next-hop router.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
[ no ] ipv6 route ipv6_address/prefix_length { interface name | next-hop ipv6_address interface name } [ cost cost ] [ precedence precedence ]
```

- **no**
  Removes the specified static route.

- **ipv6_address/prefix_length**
  Specifies a destination IPv6 address or group of addresses that will use this route.
  The `ipv6_address/prefix_length` must be specified in IPv6 colon separated notation.

- **interface name**
  Specifies the name of the interface on this system associated with the specified route or next-hop address.
  The `name` must be an existing interface name on the system and be from 1 to 79 alpha and/or numeric characters.

- **next-hop ipv6_address**
  The IPv6 address of the directly connected next hop device. The `ipv6_address` must be specified in IPv6 colon separated notation.

- **cost cost**
  Default: 0
  Defines the number of hops to the next gateway. The `cost` must be an integer value from 0 to 255.

- **precedence precedence**
  Default: 1
  Indicates the administrative preference of the route. A low precedence specifies that this route takes preference over the route with a higher precedence. The `precedence` must be an integer value from 1 to 254.

**Usage**

Use this command to create a static route and send data traffic to a next-hop device.

**Example**

Use the following example to configure a static route with ipv6 prefix/length:
```
2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24 to the next hop interface egress1:
```
ipv6 route 2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24 interface egress1
**isakmp disable-phase1-rekey**

This command is deprecated. Use `ikev1 disable-phase1-rekey` command to configure the parameters for Phase1 SA rekeying when ISAKMP lifetime expires for IKE v1 protocol.
isakmp keepalive

This command is deprecated. Use `ikev1 keepalive dpd` command to configure ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.
**isakmp policy**

This command is deprecated. Use `ikev1 policy` command to create/configure an ISAKMP policy with the specified priority for IKE v1 protocol.
iups-service

This command creates an Iu-PS service instance and enters the Iu-PS Service configuration mode. This mode defines the configuration and usage of Iu-PS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN) and defines both the control plane (GTP-C) and the data plane (GTP-U) between these nodes.

**Important:** For details about the commands and parameters for this mode, check the IuPS Service Configuration Mode chapter.

<table>
<thead>
<tr>
<th>Product</th>
<th>SGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax**

```
iups-service srvc_name
no iups-service srvc_name
```

- **no**
  - Remove the configuration for the specified Iu-PS service from the configuration for the current context.

- **srvc_name**
  - A unique string of 1 to 63 alphanumeric characters that identify the specific IuPS service.

**Usage**

Use this command to create, edit, or remove an Iu-PS service. Add up to 8 definitions to be used with a single SGSN service so the SGSN can support multiple PLMNs.

**Example**

The following command creates an Iu-PS service named iu-ps1:

```
iups-service iu-ps1
```

The following command removes the Iu-PS service named iu-ps1:

```
no iups-service iu-ps1
```
l2tp peer-dead-time

Configures a delay for attempting to tunnel to a specific peer which is initially unreachable due to reasons such as a network issue or temporarily having reached its capacity.

Product
All

Privilege
Security Administrator, Administrator

Syntax

l2tp peer-dead-time seconds

default l2tp peer-dead-time

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rests the command to it’s default setting of 60.</td>
</tr>
</tbody>
</table>

| peer-dead-time |
| seconds: Must be an integer value from 5 to 64,000. |
| Default: 60 |

Usage
The time to wait before trying to establish a tunnel to a known peer after the initial attempt was unsuccessful.

Example
The following example configures the delay in attempting to tunnel to a temporarily unreachable peer. The delay is set to 120 seconds in this example.

l2tp peer-dead-time 120
**lac-service**

Enters the lac-service configuration mode, or is used to add or remove a specified LAC service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
lac-service name

no lac-service name
```

- **no**
  Removes the specified lac-service from the current context.

- **name**
  Specifies the name of a LAC service to configure, add, or remove. It can be from 1 to 63 alpha and/or numeric characters in length and is case-sensitive.

**Usage**
Enter the LAC service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

! **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

**Example**
To add a new LAC service named LAC1 and enter the lac-service configuration mode, enter the following commands:

```plaintext
lac-service LAC1
Are you sure? [Yes|No]: Yes
```

To configure an existing LAC service named LAC2, enter the following command:

```plaintext
lac-service LAC2
```

To delete an existing LAC service named LAC3, enter the following command:

```plaintext
no lac-service LAC3
```
lma-service

Creates an Local Mobility Anchor (LMA) service or specifies an existing LMA service and enters the LMA service configuration mode for the current context.

Product
P-GW

Privilege
Administrator

Syntax

```
lma-service service_name [ -noconfirm ]
```

```
no lma-service service_name
```

**service_name**
Specifies the name of the LMA service. If `service_name` does not refer to an existing service, the new service is created if resources allow.

`service_name` must be from 1 to 63 alpha and/or numeric characters.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

```
no lma-service service_name
```

Removes the specified LMA service from the context.

Usage
Enter the LMA service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:
```
[context_name]hostname(config-lma-service)#
```

LMA Service Configuration Mode commands are defined in the LMA Service Configuration Mode Commands chapter.
Use this command when configuring the following eHRPD and PMIP SAE components: P-GW.

Example
The following command enters the existing LMA service configuration mode (or creates it if it doesn’t already exist) for the service named `lma-service1`: 
lma-service lma-service1

The following command will remove lma-service1 from the system:

no lma-service lma-service1
ins-service

Enters the lac-service configuration mode, or is used to add or remove a specified LNS service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ins-service name

no ins-service name
```

- **no**
  Removes the specified lac-service from the current context.

- **name**
  Specifies the name of a LNS service to configure, add, or remove. It can be from 1 to 63 alpha and/or numeric characters in length and is case-sensitive.

**Usage**
Enter the LNS service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

⚠️ **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

**Example**
To add a new LNS service named LNS1 and enter the ins-service configuration mode, enter the following commands:

```
ins-service LNS1
Are you sure? [Yes|No]: Yes
```

To configure an existing LNS service named LNS2, enter the following command:

```
ins-service LNS2
```

To delete an existing LNS service named LNS3, enter the following command:

```
o ins-service LNS3
```
lawful-intercept

This command defines the acknowledgement parameters for the UDP event delivery interface. It also specifies the interface IP address(es) that go into the headers of the content and event delivery messages going to the DF.

**Product**
PDSN, HA, GGSN, PDIF, SGSN, ASN-GW, SCM

**Privilege**
Security Administrator, Administrator with LI-Administrator privileges

**Syntax**

```
lawful-intercept { acked-udp [ num-retry number ] [ timeout time ] | event-attributes bsid | hand-off-policy send-start-intercept-with-pdp-active-iri | interception-point-policy { { sms-mo | sms-mt } { message-delivered | request-received } } | reprovision-target-policy resend-pdp-context-active-iri | src-ip-addr ip_address | sms-content-policy { exclude-content | include-content } | tcp tcp_option | unack-format use-service-address }
```

```
default lawful-intercept { acked-udp { num-retry | timeout } | event-attributes bsid | hand-off-policy send-start-intercept-with-pdp-active-iri | interception-point-policy { sms-mo | sms-mt } | reprovision-target-policy resend-pdp-context-active-iri | sms-content-policy | tcp tcp_option | unack-format use-service-address }
```

```
no lawful-intercept { event-attributes bsid | hand-off-policy send-start-intercept-with-pdp-active-iri | reprovision-target-policy resend-pdp-context-active-iri | src-ip-addr ip_address | tcp tcp_option | unack-format use-service-address}
```

**no**

Disables the configuration parameters for selected keyword(s) for the Lawful Intercept configuration.

**default**

Sets the behavior of command/keyword to its default setting.

**acked-udp**

Entering this keyword, enables the acknowledged-UDP interface. After enter acked-udp, one or both of the following options can be entered:

- **num-retry number**: Enter an integer between 1 and 100 to define the maximum number of retries for sending an unacknowledged message. Default is 20.
- **timeout time**: Enter an integer between 1 and 100 to define the maximum number of seconds that the system waits before retransmitting an unacknowledged message. Default is 3.

**event-attributes bsid**

This keyword enables the transmission of base-station id in event attributes for intercepted PDSN. By default this keyword is disabled.
hand-off-policy send-start-intercept-with-pdp-active-iri
This optional keyword enables a policy for hand-off in the case of ISRAU (inter-SGSN routing area update) and sends a 'start intercept' message with the PDP context LI event to the mediation server.
Default: Disabled.
This keyword is only applicable to the SGSN.

 interception-point-policy
Configures the point of interception and the time of interception for an SMS. One of the following options must be selected to specify the point of interception include:
• sms-mo: point of interception for a mobile-originated SMS
• sms-nt: point of interception for a mobile-terminated SMS
After configuring the point of interception, one of the following options must be selected to configure the point in time for the interception:
• message-delivered: intercept when the SGSN receives notification from the SMSC/MS. This is the default for either SMS-MO or SMS-MT.
• request-received: intercept when the SGSN receives the request.
This keyword is only applicable to the SGSN.

reprovision-target-policy resend-pdp-context-active-iri
Reprovisions the target identity in case of duplicates and sends a PDP context active LI IRI event to the mediation server.
This keyword is only applicable to the SGSN.
sms-content-policy {exclude-content | include-content}
This optional keyword is used to define the SMS content policy and used to configure to send only the SMS header or SMS header and content in SMS IRI event. The delivery from/to the mobile subscriber a SMS event, which contains the content and header of the SMS, is generated and sent via the Delivery Function 2 to the LEA in the same way as the IRI. LEA can configure the SMS policy if an SMS event shall contain only SMS header, or SMS header and SMS content.
Default behaviour is to send SMS header and Content in SMS IRI.
Following options can be configured:
• exclude-content: Sets the policy to send only SMS header in IRI.
• include-content: Sets the policy to send SMS header and content both in IRI.
By default it is enabled.

 src-ip-address
ip_address: This is known as the source-address. It is an IPv4 address that identifies the system’s interface, in the current context, from which the intercepted messages are forwarded to the DF according to the event delivery or content delivery provisioning done in the Exec configuration mode.

tcp tcp_option
Enables the use of TCP (in place of UDP) as the transport for sending the intercepted information to the DF.
One of the following options must be configured:
• application-heartbeat-messages timeout minute dur - In firewall enabled scenario TCP connections get dropped by because of the connections being idle most of the time. This keyword enables the SGSN to send application level heart beat messages to the mediation server to
keep connection live. This keyword is used to enable/disable sending of heartbeat messages. By default this mode is disabled

**timeout** minute duration sets the timeout duration for heartbeat timer. By default heartbeat timer value is 5 minutes.

**connection-retry-timer** time - configures the maximum time to wait before retrying to connect, in seconds. Default is 2 seconds. time: enter any integer from 1 to 65535.

**content-delivery dest-addr** ip_address - configures the destination IP address of the DF3 to send the intercepted content (ie: data/CC). ip_address: enter an address in standard IPv4/IPv6 format. Must be followed by:

  **dest-port** port_num - configures the destination port where the intercepted information is to be forwarded. port_num: enter any integer from 1 to 65535.

**event-delivery dest-addr** ip_address - configures the destination address of the DF2 to send the intercepted events information (ie: IRI). ip_address: enter an address in standard IPv4/IPv6 format. Must be followed by:

  **dest-port** port_num - configures the destination port where the intercepted information is to be forwarded. port_num: enter any integer from 1 to 65535.

**unack-format use-service-address**

This set of keywords instructs the system to use the service-address, in place of the source-address in the ip-headers of the intercepted messages that are forwarded to the DF according to the content delivery provisioning done in the Exec configuration mode. The service-address is an IPv4 address that identifies on which of the system’s interfaces the intercept was received.

**Important:** This function requires that the Lawful Intercept provisioning (done in the Exec configuration mode) include the **udp-unack-format-1** for the **content delivery** keyword. Changing the configuration and the provisioning to enable/disable this feature can be done on the fly.

**Usage**

Use this command to configure the parameters controlling the forwarding of the intercepted messages to the DF.

For details on provisioning the Lawful Intercepts, refer to the Exec configuration mode.

For details on using the Lawful Intercept capability of the system, refer to System Administration and Configuration Guide.

**Important:** When monitoring for calls that are not yet active, the source-address information does not need to be configured immediately. However, it must be configured as soon as the call becomes active in order for Lawful Interception to function properly.

**Example**

To set the source-address in the current context to 198.162.100.10, use the following command:

```plaintext
lawful-intercept src-ip-addr 198.162.100.10
```
lawful-intercept dictionary

This command configures LI dictionary to support customer specific LI requirements.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
lawful-intercept dictionary {standard | cust_dict }
[default] lawful-intercept dictionary
```

- **default**
  Sets the LI dictionary to default; i.e. `standard`.

- **standard**
  Specifies the standard dictionary to be used for LI session.

- **cust_dict**
  Specifies the customer specific dictionaries: `custom1` through `custom10`, to be used to provision/interception for configured LI context.

**Usage**

Use this command to configure the LI dictionary to be used for LI requirements. LI dictionaries are context specific and will be applicable to provisions / interceptions for configured LI context.

**Example**

The following command specifies the standard LI dictionary to be used for LI requirements:

```
default lawful-intercept dictionary
```
mobile-ip ha reconnect

Sets the behavior of all HA services to reconnect dropped calls.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

mobile-ip { ha reconnect [ static-homeaddr [ dynamic-pool-allocation ] ] }  
no mobile-ip { ha reconnect [ static-homeaddr [ dynamic-pool-allocation ] ] }

static-homeaddr
The home address is a static IP address.

dynamic-pool-allocation
Allows a dynamic pool to accept a static address allocation.

Usage
Use this command to reset the HA behavior for new calls.

Example

mobile-ip ha reconnect

mobile-ip ha reconnect static-homeaddr

mobile-ip ha reconnect static-homeaddr dynamic-pool-allocation

no mobile-ip ha reconnect

no mobile-ip ha reconnect static-homeaddr
**mag-service**

Creates an Mobile Access Gateway (MAG) service or specifies an existing MAG service and enters the MAG service configuration mode for the current context.

**Product**
HSGW, S-GW

**Privilege**
Administrator

**Syntax**

```plaintext
mag-service service_name [ -noconfirm ]
```

*service_name*

Specifies the name of the MAG service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

*service_name* must be from 1 to 63 alpha and/or numeric characters.

```plaintext
-noconfirm
```

Indicates that the command is to execute without any additional prompt and confirmation from the user.

```plaintext
no mag-service service_name
```

Removes the specified MAG service from the context.

**Usage**

Enter the MAG service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mag-service)#
```

MAG Service Configuration Mode commands are defined in the MAG Service Configuration Mode Commands chapter.

Use this command when configuring the following eHRPD and PMIP SAE components: HSGW and S-GW.

**Example**

The following command enters the existing MAG service configuration mode (or creates it if it doesn’t already exist) for the service named *mag-service1*:
mag-service mag-service1

The following command will remove mag-service1 from the system:

no mag-service mag-service1
map-service

This command creates a Mobile Application Part (MAP) Service instance and enters the MAP Service configuration mode to define or edit the MAP service parameters.

MAP is the SS7 protocol that provides the application layer required by some of the nodes in GPRS/UMTS networks to communicate with each other in order to provide services to mobile phone users. MAP is used by the serving GPRS support node (SGSN) to access SS7 network nodes such as a home location register (HLR) or a radio access network (RAN).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
map-service srvc_name

no map-service srvc_name
```

**Usage**
Use this command to create, edit, or remove a MAP service configuration.

**Important:** For details about the commands and parameters, check the MAP Service Configuration Mode chapter.

**Example**
The following command creates a MAP service named map-1:

```
map-service map-1
```

The following command removes the configuration for a MAP service named map-1 from the configuration for the current context:

```
no map-service map-1
```
mme-hss-service

Creates an Mobility Management Entity (MME)-HSS service or configures an existing MME HSS service and enters the MME-HSS service configuration mode for EPC network in the current context.

Product
MME

Privilege
Administrator

Syntax

mme-hss-service service_name [-noconfirm]

no mme-hss-service service_name

service_name
Specifies the name of the MME HSS service. If service_name does not refer to an existing service, the new service is created if resources allow.

-service_name must be from 1 to 63 alpha and/or numeric characters.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Enter the MME HSS service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

[context_name]hostname(config-mme-hss-service)#

MME HSS Service Configuration Mode commands are defined in the MME HSS Service Configuration Mode Commands chapter.
Use this command when configuring the eGTP SAE component(s); i.e. MME.

Example

The following command enters the existing MME HSS service configuration mode (or creates it if it doesn’t already exist) for the service named mme-hss-service1:
**mme-hss-service** *mme-hss-service1*

The following command will remove *mme-hss-service1* from the system:

```
no mme-hss-service mme-hss-service1
```
mme-service

Creates an Mobility Management Entity (MME) service or configures an existing MME service and enters the MME service configuration mode for EPC networks in the current context.

Product
MME

Privilege
Administrator

Syntax

mme-service service_name [-noconfirm]
no mme-service service_name

**no**
Removes the specified MME service from the context.

**service_name**
Specifies the name of the MME service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

*service_name* must be from 1 to 63 alpha and/or numeric characters.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Enter the MME service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 8 MME service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

⚠️ **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:
[context_name]hostname(config-mme-service)#
MME Service Configuration Mode commands are defined in the MME Service Configuration Mode Commands chapter.

⚠️ **Caution:** This is a critical configuration. The MME service can not be configured without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.
Example
The following command enters the existing MME service configuration mode (or creates it if it doesn’t already exist) for the service named \textit{mme-service1}:

\texttt{mme-service mme-service1}

The following command will remove \textit{mme-service1} from the system:

\texttt{no mme-service mme-service1}
mobile-ip

The commands in this section are used for configuring mobile IP parameters.
**mobile-ip fa newcall**

Configures settings that effect all FA services in the current context.

**Product**
FA

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
mobile-ip fa { multiple-dynamic-reg-per-nai | newcall duplicate-home-address } { accept | reject }

no mobile-ip fa { multiple-dynamic-reg-per-nai | newcall duplicate-home-address }
```

**Usage**
Use this command to set the behavior of all FA services in the current context.

**Example**
To configure all FA services to accept new calls and drop the existing call when the new call requests an IP address that is already in use by an existing call, enter the following command:

```
mobile-ip fa newcall duplicate-home-address accept
```

To enable all FA services in the current context to allow all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI, enter the following command:

```
mobile-ip fa multiple-dynamic-reg-per-nai
```
mobile-ip ha assignment-table

This command creates a Mobile IP HA assignment table and enters Mobile IP HA Assignment Table Configuration Mode.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mobile-ip ha assignment-table atable_name[-noconfirm]
```

```
no mobile-ip ha assignment-table atable_name
```

- **no**
  This keyword deletes the specified assignment table

- **atable_name**
  The name of the MIP HA assignment table to create or edit.

- **-noconfirm**
  This keyword specifies that the assignment table should be created with no further confirmation by the user.

**Usage**

Use this command to create a new MIP HA assignment table or edit an existing MIP HA assignment table.

**Important**: A maximum of 8 MIP HA assignment tables can be configured per context with a maximum of 8 MIP HA assignment tables across all contexts.

**Important**: A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

**Example**
The following command creates a new MIP HA assignment table name MIPHAtable1 and enters MIP HA Assignment Table configuration mode without asking for confirmation from the user:

```
mobile-ip ha assignment-table MIPHAtable1
```
mobile-ip ha newcall

Configures the behavior of all HA services when duplicate home addresses and duplicate IMSI sessions occur for new calls.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
mobile-ip ha newcall { duplicate-home-address { accept | reject } | duplicate-imsi-session { allow | disallow | global-disallow } }

no mobile-ip ha newcall { duplicate-home-address | duplicate-imsi-session }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mobile-ip ha newcall</code></td>
<td>Configures the behavior of all HA services for new calls.</td>
</tr>
<tr>
<td><code>duplicate-home-address</code></td>
<td>Reset the option to it’s default of reject.</td>
</tr>
<tr>
<td><code>duplicate-imsi-session</code></td>
<td>Reset the option to its default of allow.</td>
</tr>
<tr>
<td><code>accept</code></td>
<td>Configures the HA to either accept or reject new calls if the new call requests a static IP home address that is already assigned to an existing call from an IP address pool in the same destination context. The new call is accepted and the existing call is dropped.</td>
</tr>
<tr>
<td><code>reject</code></td>
<td>Configures the HA to either permit or not permit multiple sessions for the same IMSI. If a Mobile node already has an active session and a new sessions is requested using the same IMSI, the currently active session is dropped and the new session is accepted. Enables HA services in this context to accept a new session and disconnect any other session(s) having the same IMSI being processed in this context. In addition, a request is sent to all other contexts containing HA services to do the same.</td>
</tr>
</tbody>
</table>

**Important:** In order to ensure a single session per IMSI across all contexts containing HA services, the global-disallow option must be configured in every context.

**Usage**

Use this command to set the behavior of all HA services for new calls.
Example
To configure all HA services to accept new calls when the new call requests a static IP that is already assigned from an IP pool in the same destination context, enter the following command:

`mobile-ip ha newcall duplicate-home-address accept`

To configure all HA services to drop an active call and accept a new one that uses the same IMSI, enter the following command:

`mobile-ip ha newcall duplicate-imsi-session disallow`
mobile-ip ha reconnect

Sets the behavior of all HA services to reconnect dropped calls.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
mobile-ip { ha reconnect [ static-homeaddr [ dynamic-pool-allocation ] ] } 
no mobile-ip { ha reconnect [ static-homeaddr [ dynamic-pool-allocation ] ] } 
```

```
static-homeaddr
The home address is a static IP address.

dynamic-pool-allocation
Allows a dynamic pool to accept a static address allocation.
```

Usage
Use this command to reset the HA behavior for new calls.

Example

```
mobile-ip ha reconnect
mobile-ip ha reconnect static-homeaddr
mobile-ip ha reconnect static-homeaddr dynamic-pool-allocation
no mobile-ip ha reconnect
no mobile-ip ha reconnect static-homeaddr
```
mpls bgp forwarding

This command globally enables the MPLS BGP forwarding.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[no] mpls bgp forwarding

no

Disables MPLS BGP forwarding configured on the system.

Usage
Use this command to globally enable the MPLS BGP forwarding. By enabling this command, the BGP VPNv4 routes need not have an underlying LSP to forward the IP packets. If this command is not enabled, then the nexthop for the BGP routes must be reachable via LDP.

⚠️Caution: This command should be enabled ONLY when all the BGP peering where VPNv4 routes are exchanged are one hop away.

Example
Following command enables the MPLS BGP forwarding on system:

mpls bgp forwarding
nw-reachability server

This command adds/deletes a reachability-detect server and configures parameters for retrying the failure-detection process. When network reachability is enabled, a ping request is sent to this device. If there is no response after a specified number of retries, the network is deemed failed. Execute this command multiple times to configure multiple network reachability servers.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

nw-reachabilityserver server_name [ interval seconds ] [ local-add ip_addr ] [ num-retry num ] [ remote-add ip_addr ] [ timeout seconds ]

nw-reachabilityserver server_name

no
Delete the reference to the specified network reachability server.

server_name
A name for the network device that is sent ping packets to test for network reachability.

interval seconds
Default: 60 seconds
Specifies the frequency in seconds for sending ping requests. seconds must be an integer from 1 through 3600.

local-add ip_addr
Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. ip_addr must be an IP v4 address in dotted decimal notation.

num-retry num
Default: 5
Specifies the number of retries before deciding that there is a network-failure. num must be an integer from 0 through 100.

remote-add ip_addr
Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. ip_addr must be an IP v4 address in dotted decimal notation.

timeout seconds
Default: 3 seconds
Specifies how long to wait, in seconds, before retransmitting a ping request to the remote address. *seconds* must be an integer from 1 through 10.

**Usage**

Use this command to set up a network device on a destination network that is used to ensure that Mobile IP sessions can reach the required network from the HA.

**Important:** Refer to the HA configuration mode command `policy nw-reachability-fail` to configure the action that should be taken when network reachability fails.

**Important:** Refer to the subscriber config mode command `nw-reachability-server` to bind the network reachability to a specific subscriber.

**Important:** Refer to the `nw-reachability server server_name` keyword of the `ip pool` command in this chapter to bind the network reachability server to an IP pool.

**Example**

To set a network device called InternetDevice with the IP address of 192.168.100.10 as the remote address that is pinged to determine network reachability and use the address 192.168.200.10 as the origination address of the ping packets sent, enter the following command:

```
 nw-reachability server InternetDevice local-addr 192.168.200.10 remote-addr 192.168.100.10
```
network-requested-pdp-context

The commands in this section are used for configuring Network Requested PDDP Context functionality.
network-requested-pdp-context activate

Configures the mobile station(s) (MSs) for which network initiated PDP contexts are supported.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

network-requested-pdp-context activate address ip_address dst-context context_name imsi imsi apn apn_name
nenetwork-requested-pdp-context activate{ address ip_address dst-context context_name}

no
Disables the system’s ability to accept network-requested PDP contexts on the specified interface.

dst-context context_name
Specifies the destination context configured on the system containing the static IP address pool in which the MS’s IP address is configured.
context_name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.

imsi imsi
Specifies the International Mobile Subscriber Identity (IMSI) of the MS.
imsi must be from 1 to 15 numeric characters.

apn apn_name
Specifies the Access Point Name (APN) that is passed to the SGSN by the system.
apn_name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Usage
Use this command to specify the MS(s) for which network initiated PDP contexts are supported.
When a packet is received for an MS that does not currently have a PDP context established, the system checks the configuration of this parameter to determine if the destination IP address specified in the packet is specified by this parameter. If the address is not specified, then the system discards the packet. If the address is specified, the system uses the configured IMSI and APN to determine the appropriate SGSN from the Home Location Register (HLR). The system communicates with the HLR through the interworking node configured using the network-requested-pdp-context gsn-map command.
Once the session is established, the destination context specified by this command is used in place of the one either configured within the specified APN template or returned by a RADIUS server during authentication.
network-requested-pdp-context activate

This command can be issued multiple times supporting network initiated PDP contexts for up to 1000 configured addresses per system context.

Example
The following command enables support for network initiated PDP contexts for an MS with a static IP address of 20.13.5.40 from a pool configured in the destination context pdn1 with an IMSI of 3319784450 that uses an APN template called isp1:

```
network-requested-pdp-context activate address 20.13.5.40 dst-context pdn1 imsi 3319784450 apn isp1
```
network-requested-pdp-context gsn-map

Configures the IP address of the interworking node that is used by the system to communicate with the HLR and optionally sets the GTP version to use.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

network-requested-pdp-context gsn-map [ ip_address [ gtp-version { 0 | 1 } ] ]

nonetwork-requested-pdp-context gsn-map

no
Deletes a previously configured gsn-map node.

ip_address
Specifies the IP address of the gsn-map node. ip_address must be an IPv4 or IPv6 IP address entered using dotted decimal notation or an IPv6 IP address using colon (:) separated notation.

[gtp-version { 0 | 1 } ]
Default: 1
Specifies the gtp version used.

Usage
Communications from the system to the HLR must go through a GSN-map interworking node that performs the protocol conversion from GTPC to SS7. The UDP port for this communication is 2123. Support for network requested PDP contexts must be configured within source contexts on the system. Only one gsn-map node can be configured per source context. The source context also contains the GGSN service configuration that specifies the IP address of the Gn interface. If multiple GGSN services are configured in the source context, one is selected at random for initiating the Network Requested PDP Context Activation procedure. Communication with the gsn-map node is done over the Gn interface configured for the GGSN service. The IP address of that interface is used as the system’s source address.

Example
The following command configures the system to communicate with a gsn-map node having an IP address of 192.168.2.5:

network-requested-pdp-context gsn-map 192.168.2.5
network-requested-pdp-context hold-down-time

Configures the time duration to that the system will wait after the SGSN rejects an attempt for a network-requested PDP context creation for the subscriber.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
network-requested-pdp-context hold-down-time time
```

`time`
Default: 60
The time interval is measured in seconds and can be configured to any integer value between 0 and 86400.

Usage
Packets received during this time period would be discarded, rather than being used to cause another network-requested PDP context creation attempt for the same subscriber. After the time period has expired, any subsequent packets received would cause another network-requested PDP context creation procedure to begin.

Example
The following command configures a hold-down-time of 120 seconds:

```
network-requested-pdp-context hold-down-time 120
```
network-requested-pdp-context interval

Configures the minimum amount of time that must elapse between the deletion of a network initiated PDP context and the creation of a new one for the same MS.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
network-requested-pdp-context interval time
```

<table>
<thead>
<tr>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 60</td>
</tr>
<tr>
<td>Specifies the minimum amount of time that must pass before the system allows another network-requested PDP context for a specific MS after the previous context was deleted.</td>
</tr>
<tr>
<td>$time$ is measured in seconds and can be configured to any integer value from 0 to 86400.</td>
</tr>
</tbody>
</table>

Usage

Once an MS deletes a PDP context that initiated from the network, the system automatically waits the amount of time configured by this parameter before allowing another network initiated PDP context for the same MS.

Example

The following command specifies that the system waits 120 seconds before allowing another network requested PDP context for an MS:

```
network-requested-pdp-context interval 120
```
network-requested-pdp-context sgsn-cache-time

Configures the time duration that the GGSN keeps the SGSN/subscriber pair cached in its local memory.

Product  
GGSN

Privilege  
Security Administrator, Administrator

Syntax

```
network-requested-pdp-context sgsn-cache-time <time>
```

```
time
Default: 300
The time interval is measured in seconds and can be configured to any integer value between 0 and 86400.
```

Usage

For an initial network-requested PDP context creation, the system contacts the HLR (via the GSN-MAP interworking node) to learn which SGSN is currently servicing the subscriber. The system keeps that information in cache memory for the configured time, so that future network-requested PDP context creations for that subscriber can be initiated without having to contact the HLR again.

Example

The following command configures an sgsn-cache-time of 500 seconds:

```
network-requested-pdp-context sgsn-cache-time 500
```
operator

Configures a context-level operator account within the current context.

Product
All

Privilege
Security Administrator

Syntax

operator user_name [ encrypted ] password pwd [ ecs ] [ expiry-date date_time ] [ li-administration ] [ noecs ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [ timeout-idle idle_seconds ] [ timeout-min-idle idle_minutes ]

no operator user_name

no

Removes a previously configured context-level operator account.

user_name

Specifies a name for the account. user_name must be from 1 to 32 alpha and/or numeric characters.

[ encrypted ] password pwd

Specifies the password to use for the user which is being given context-level operator privileges within the current context. The encrypted keyword indicates the password specified uses encryption. The password specified as pwd must be from 1 to 63 alpha and/or numeric characters without encryption and must be from 1 to 127 alpha and/or numeric characters when encryption has been indicated. The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted password keyword in the configuration file as a flag that the variable following the encrypted password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

cacs

Default: ACS-specific configuration commands not allowed. Permits the specific user to access ACS-specific configuration commands from Executive mode only.

expiry-date date_time

The date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

li-administration

Permits this user to execute Lawful Intercept commands.
**Important:** Users who have Lawful Intercept privileges are only given those privileges when connected to the system through a Secure Shell (SSH). If this user connects through a Telnet session or through the console port, Lawful Intercept privileges are not enabled.

**noecs**
Default: Enabled.
Prevents the specific user to access ACS-specific configuration commands.

**timeout-absolute abs_seconds**
Default: 0
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of time, in seconds, the context-level operator may have a session active before the session is forcibly terminated. abs_seconds must be a value in the range from 0 through 300000000.
The special value 0 disables the absolute timeout.

**timeout-min-absolute abs_minutes**
Default: 0
Specifies the maximum amount of time, in minutes, the context-level operator may have a session active before the session is forcibly terminated. abs_minutes must be a value in the range from 0 through 300000000.
The special value 0 disables the absolute timeout.

**timeout-idle idle_seconds**
Default: 0
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of idle time, in seconds, the context-level operator may have a session active before the session is terminated. idle_seconds must be an integer from 0 through 300000000.
The special value 0 disables the idle timeout.

**timeout-min-idle idle_minutes**
Default: 0
Specifies the maximum amount of idle time, in minutes, the context-level operator may have a session active before the session is terminated. idle_minutes must be a value in the range from 0 through 300000000.
The special value 0 disables the idle timeout.

**Usage**
Create new context-level operator or modify existing operator’s options, in particular, the timeout values. Operator users have read-only privileges. They can maneuver across multiple contexts, but cannot perform configuration operations. Refer to the Command Line Interface Overview chapter of this guide for more information.

**Important:** A maximum of 128 administrative users and/or subscribers may be locally configured per context.
Example
The following command creates a context-level operator account called user1 with ACS parameter control:

    operator user1 password secretPassword ecs

The following command removes a previously configured context-level operator account called user1:

    no operator user1
optimize pdsn inter-service-handoff

Controls the optimization of the system’s handling of inter-PDSN handoffs.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
optimize pdsn inter-service-handoff

[ default | no ] optimize pdsn inter-service-handoff
```

- **default**
  
  Resets the command to it’s default setting of enabled.

- **no**
  
  Disables the feature.

**Usage**

When more than one PDSN service is defined in a context, each PDSN-Service acts as an independent PDSN. When a Mobile Node (MN) moves from one PDSN service to another PDSN service, by rule, it is an inter-PDSN handoff. This command optimizes PDSN handoffs between PDSN Services that are defined in the same context in the system.

The default for this parameter is enabled. The no keyword disables this functionality.

When enabled, the system treats handoffs happening between two PDSN services in the same context as an inter-PDSN handoff. Existing PPP session states and connection information is reused. If the inter-PDSN handoff requires a PPP restart, then PPP is restarted. The optimized inter-service-handoff may not restart the PPP during handoffs allowing the MN to keep the same IP address for the Simple IP session.

**Example**

```
optimize pdsn inter-service-handoff
```
pdg-service

Creates a new PDG service or specifies an existing PDG service and enters the PDG Service Configuration Mode. A maximum of 16 PDG services can be created. This limit applies per ASR 5000 chassis and per context.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Syntax

```
  pdg-service name
  no pdg-service name
```

**pdg-service name**

Specifies the name of a new or existing PDG service.

*name* must be from 1 to 63 alpha and/or numeric characters and must be unique across all FNG services within the same context and across all contexts.

**no pdg-service name**

Deletes the specified PDG service.

Usage

Use this command in Context Configuration Mode to create a new PDG service or modify an existing one. Executing this command enters the PDG Service Configuration Mode.

Example

The following command configures an PDG service named *pdg_service_1* and enters the PDG Service Configuration Mode:

```
pdg-service pdg_service_1
```
pdif-service

Creates a new, or specifies an existing, PDIF service and enters the PDIF Service Configuration Mode.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

[ no ] pdif-service name [ -noconfirm ]

name
Specifies the name of a new or existing PDIF service. name must be from 1 to 63 alpha and/or numeric characters.

Usage
Use this command to create a new or enter an existing PDIF service.
Entering this command results in the following prompt:
[context_name]hostname(config-pdif-service)#
PDIF Service Configuration Mode commands are defined in the PDIF Service Configuration Mode Commands chapter.

Example
The following command configures a PDIF service called pdif2 and enters the PDIF Service Configuration Mode:

pdif-service pdif2
pdsn-service

Creates/deletes a packet data service or specifies an existing PDSN service for which to enter the packet data service configuration mode for the current context.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

    pdsn-service name

    no pdsn-service name

    no
    Indicates the packet data service specified is to be removed.

    name
    Specifies the name of the PDSN service to configure. If name does not refer to an existing service, the new service is created if resources allow. name must be from 1 to 63 alpha and/or numeric characters.

Usage
Enter the PDSN service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

⚠️ Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example
The following command will enter the PDSN service configuration mode creating the service sampleService, if necessary.

    pdsn-service sampleService

The following command will remove sampleService as being a defined PDSN service.

    no pdsn-service sampleService
pgw-service

Creates an P-GW service or specifies an existing P-GW service and enters the P-GW service configuration mode for the current context.

Product
P-GW

Privilege
Administrator

Syntax

```
pgw-service service_name [ -noconfirm ]
```

```
no pgw-service service_name
```

`service_name`
Specifies the name of the P-GW service. If `service_name` does not refer to an existing service, the new service is created if resources allow.

`service_name` must be from 1 to 63 alpha and/or numeric characters.

```
-noconfirm
```
Indicates that the command is to execute without any additional prompt and confirmation from the user.

```
no pgw-service service_name
```
Removes the specified P-GW service from the context.

Usage
Enter the P-GW service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

⚠️ Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:
```
[context_name]hostname(config-pgw-service)#
```
P-GW Service Configuration Mode commands are defined in the P-GW Service Configuration Mode Commands chapter.
Use this command when configuring the following eHRPD and SAE components: P-GW.

Example
The following command enters the existing P-GW service configuration mode (or creates it if it doesn’t already exist) for the service named `pgw-service1`:
The following command will remove `pgw-service1` from the system:

```
no pgw-service pgw-service1
```
**policy**

Enters an existing accounting policy or creates a new one where accounting parameters are configured.

**Product**
HSGW, P-GW, S-GW

**Privilege**
Administrator

**Syntax**

```
[no] policy accounting name
```

- **no**
  Removes the specified accounting policy from the context.

- **name**
  Specifies the name of the existing or new accounting policy. *name* must be from 1 to 63 alpha and/or numeric characters.

**Usage**

Use this command to enter the Accounting Policy Configuration mode to edit an existing accounting policy or configure a new policy.

Entering this command results in the following prompt:
```
[context_name]hostname(config-accounting-policy)#
```

Accounting Policy Configuration Mode commands are defined in the Accounting Policy Configuration Mode Commands chapter.

**Example**

The following command enters the Accounting Policy Configuration Mode for a policy named acct5:

```
policy accounting acct5
```
**policy-group**

This command deletes/creates and enters the Policy-Group configuration mode within the current destination context for flow-based traffic policing to a subscriber session flow.

**Product**

PDSN, HA, ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] policy-group name policy_group
```

- **no**
  Deletes configured policy group within the context.

- **policy_group**
  Specifies the name of Policy-Group and can consist of from 1 to 15 alpha and/or numeric characters in length and is case sensitive.

**Usage**

Use this command to form a policy group from a set of configured Policy-Maps. A policy group supports up to 16 policies for a subscriber session flow.

**Example**

Following command configures a policy group policy_group1 for a subscriber session flow.

```plaintext
policy-group name policy_group1
```
**policy-map**

This command deletes/creates and enters the Traffic Policy-Map configuration mode within the current destination context to configure the flow-based traffic policing for a subscriber session flow.

**Product**
PDSN, HA, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] policy-map name policy_name
```

- **no**
  
  Deletes configured Policy-Map within the context.

- **policy_name**
  
  Specifies the name of Policy-Map and must consist of from 1 to 15 alpha and/or numeric characters in length and is case sensitive.

**Usage**

Use this command to enter Traffic Policy-Map configuration mode and to set the Class-Map and corresponding traffic flow treatment to traffic policy for a subscriber session flow.

**Example**

Following command configures a policy map policy1 w where other flow treatments is configured.

```
policy-map name policy1
```
**Context Configuration Mode Commands**

**ppp**

Configures point-to-point protocol parameters for the current context.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ppp { acfc { receive { allow | deny } | transmit { apply | ignore | reject } } | auth-retry-suppress-aaa-auth | chap fixed-challenge-length length | dormant send lcp-terminate | echo-max-retransmissions num_retries | echo-retransmit-timeout msec | first-lcp-retransmit-timeout milliseconds | lcp-authentication discard retry-alternate num_discard | lcp-authentication-reject retry-alternate | lcp-start-delay delay | lcp-terminate connect-state | lcp-terminate mip-lifetime-expiry | lcp-terminate mip-revocation | max-authentication-attempts num | max-configuration-nak num | max-retransmissions number | max-terminate number | mru-packet-size | negotiate default-value-options | peer-authentication user_name [ encrypted ] password [ password ] | pfc { receive { allow | deny } | transmit { apply | ignore | reject } } | reject-peer-authentication | renegotiation retain-ip-address | retransmit-timeout milliseconds }
no ppp { auth-retry-suppress-aaa-auth | chap fixed-challenge-length | dormant send lcp-terminate | lcp-authentication discard retry-alternate num_discard | lcp-authentication-reject retry-alternate | lcp-start-delay | lcp-terminate connect-state | reject-peer-authentication | renegotiation retain-ip-address }
default lcp-authentication discard retry-alternate num_discard
```

**default**

Restores the system defaults for the specific command/keyword.

```plaintext
```

Disables, deletes, or resets the specified option.

In case of **no ppp renegotiation retain-ip-address**, the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

```plaintext
acfc { receive { allow | deny } | transmit { apply | ignore | reject } }
```

Configures PPP Address and Control Field Compression (ACFC) parameters.

```plaintext
receive { allow | deny }
```

Default: allow
This keyword specifies whether to allow Address and Control Field Compressed PPP packets received from the Peer. During LCP negotiation, the local PPP side indicates whether it can handle ACFC compressed PPP packets.

When allow is specified, the local PPP side indicates that it can process ACFC compressed PPP packets and compressed packets are allowed. When deny is specified, the local PPP side indicates that it cannot handle ACFC compressed packets and compressed packets are not allowed.

```
transmit { apply | ignore | reject }
```

Default: ignore

Specifies how Address and Control Field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle ACFC compressed PPP packets. When apply is specified, if the peer requests ACFC, the request is accepted and ACFC is applied for transmitted PPP packets. When ignore is specified, if the peer requests ACFC, the request is accepted, but ACFC is not applied for transmitted PPP packets. When reject is specified, if the peer requests ACFC, the request is rejected and ACFC is not applied to transmitted packets.

```
auth-retry suppress-aaa-auth
```

Default: no auth-retry suppress-aaa-auth

This option does not allow PPP authentication retries to the AAA server after the AAA server has already authenticated a session. PPP locally stores the username and password, or challenge response, after a successful PPP authentication. If the Mobile Node retries the PAP request or CHAP-Response packet to the PDSN, PPP locally compares the incoming username, password or Challenge Response with the information stored from the previous successful authentication. If it matches, PAP ACK or CHAP Success is sent back to the Mobile Node, without performing AAA authentication. If the incoming information does not match with what is stored locally, then AAA authentication is attempted. The locally stored PPP authentication information is cleared once the session reaches a connected state.

**Important:** This option is not supported in conjunction with the GGSN product.

```
chap fixed-challenge-length length
```

Default: Disabled. PAP CHAP uses a random challenge length.

Normally PPP CHAP uses a random challenge length from 17 to 32 bytes. This command allows you to configure a specific fixed challenge length of from 4 through 32 bytes.

```
length must be an integer from 4 through 32.
```

```
dormant send-lcp-terminate
```

Indicates a link control protocol (LCP) terminate message is enabled for dormant sessions.

**Important:** This option is not supported in conjunction with the GGSN product.

```
echo-max-retransmissions num_retries
```

Default: 3

Configures the maximum number of retransmissions of LCP ECHO_REQ before a session is terminated in an always-on session.

```
um_retries must be a value in the range of 1 to 16.
```

```
echo-retransmit-timeout msec
```

Default: 3000
Configures the timeout, in milliseconds, before trying LCP ECHO_REQ for an always-on session. 
msec must be a value in the range of 100 to 5000.

```
first-lcp-retransmit-timeout milliseconds
```
Default: 3000
Specifies the number of milliseconds to wait before attempting to retransmit control packets. This value 
configures the first retry. All subsequent retries are controlled by the value configured for the ppp 
retransmit-timeout keyword.
milliseconds must be a value in the range 100 through 5000.

```
lcp-authentication-discard retry-alternate num_discard
```
Default: Disabled.
This keyword sets the number of discards up to which authentication option is discarded during LCP 
negotiation and retries starts to allow alternate authentication option.
um_discard must be an integer from 0 through 5. Recommended value is 2.

```
lcp-authentication-reject retry-alternate
```
Default: Disabled. No alternate authentication option will be retried.
The action that is taken if the authentication option is rejected during LCP negotiation and retry the allowed 
alternate authentication option.

```
lcp-start-delay delay
```
Default: 0
The delay in milliseconds before link control protocol (LCP) is started. delay must be an integer from 0 
through 5000.

```
lcp-terminate connect-state
```
This option enables sending an LCP terminate message to the Mobile Node when a PPP session is 
disconnected if the PPP session was already in a connected state.
Note that if the no keyword is used with this option, the PDSN must still send LCP Terminate in the event of 
an LCP/PCP negotiation failure or PPP authentication failure, which happens during connecting state.

**Important:** This option is not supported in conjunction with the GGSN product.

```
lcp-terminate mip-lifetime-expiry
```
This option configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to 
MIP Lifetime expiry (default).
Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when 
a MIP session is terminated due to MIP Lifetime expiry.

```
lcp-terminate mip-revocation
```
This option configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to 
a Revocation being received from the HA (default).
Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when 
a MIP session is terminated due to a Revocation being received from the HA.
### max-authentication-attempts num

Default: 1
Configures the maximum number of time the PPP authentication attempt is allowed. num must be an integer in the range from 1 through 10.

### max-configuration-nak num

Default: 10
This command configures the maximum number of consecutive configuration REJ/NAKs that can be sent during CP negotiations, before the CP is terminated. num must be an integer in the range from 1 through 20.

### max-retransmission number

Default: 5
Specifies the maximum number of times control packets will be retransmitted. number must be a value from 1 to 16.

### max-terminate number

Default: 2
Sets the maximum number of PPP LCP Terminate Requests transmitted to the Mobile Node. number must be an integer from 0 through 16.

**Important:** This option is not supported in conjunction with the GGSN product.

### mru packet_size

Default: 1500
Specifies the maximum packet size that can be received in bytes. packet_size must be an integer from 128 to 1500.

### negotiate default-value-options

Default: Disabled
Enable the inclusion of configuration options with default values in PPP configuration requests. The PPP standard states that configuration options with default values should not be included in Configuration Request (LCP, IPCP etc) packets. If the option is missing in the Configuration Request, the peer PPP assumes the default value for that configuration option. When negotiate default-value-options is enabled, configuration options with default values are included in the PPP configuration Requests.

### peer-authenticate user_name [ [ encrypted ] password password ]

Specifies the user name and an optional password required for point-to-point protocol peer connection authentications. user_name must be from 1 to 63 alpha and/or numeric characters. The keyword password is optional and if specified password must be from 1 to 63 alpha and/or numeric characters. The password specified must be in an encrypted format if the optional keyword encrypted was specified. The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
Context Configuration Mode Commands

pfc { receive { allow | deny } | transmit { apply | ignore | reject } }

Configures Protocol Field Compression (PFC) parameters.

receive { allow | deny }
Default: allow
This keyword specifies whether to allow Protocol Field Compression (PFC) for PPP packets received from the Peer. During LCP negotiation, the local PPP side indicates whether it can handle Protocol Field Compressed PPP packets.
When allow is specified, the peer is allowed to request PFC during LCP negotiation. When deny is specified, the Peer is not allowed to request PFC during LCP negotiation.

transmit { apply | ignore | reject }
Default: ignore
This keyword specifies how Protocol field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle PFC compressed PPP packets.
When apply is specified, if the peer requests PFC, it is accepted and PFC is applied for transmitted PPP packets. When ignore is specified, If the peer requests PFC, it is accepted but PFC is not applied for transmitted packets. When reject is specified, all requests for PCF from the peer are rejected.

reject-peer-authentication
Default: Enabled
If disabled, re-enables the system to reject peer requests for authentication.

renegotiation retain-ip-address
Default: Enabled
If enable retain the currently allocated IP address for the session during PPP renegotiation (Simple IP) between FA and Mobile node.
If disabled, the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

retransmit-timeout milliseconds
Default: 3000
Specifies the number of milliseconds to wait before attempting to retransmit control packets.
milliseconds must be a value in the range 100 through 5000.

Usage
Modify the context PPP options to ensure authentication and communication for PPP sessions have fewer dropped sessions.

Example
The following commands set various PPP options.

ppp dormant send-lcp-terminate
ppp max-retransmission 3
ppp peer-authenticate user1 password secretPwd
ppp peer-authenticate user1
**context Configuration Mode Commands**

The following command disables the sending of LCP terminate messages for dormant sessions.

```
no ppp dormant send-lcp-terminate
```
**ppp magic-number**

This command manages magic number checking during LCP Echo message handling.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ppp magic-number receive ignore
[ no | default ] ppp magic-number receive ignore
```

- **no**
  Disable the specified behavior.

- **default**
  Restores the system defaults for the specific command/keyword.

- **receive ignore**
  Default: Disabled.
  Ignores the checking of magic number at PDSN during LCP Echo message handling.
  If a valid magic numbers were negotiated for the PPP endpoints during LCP negotiation and LCP Echo Request/Response have invalid magic numbers, enabling of this command will ignore the checking of magic number during LCP Echo message handling.

**Usage**

Use this command to allow the system to ignore invalid magic number during LCP Echo Request/Response handling.

**Example**
The following command allows the invalid magic number during LCP Echo Request/Response negotiation:

```plaintext
ppp magic-number receive ignore
```
ppp statistics

This command changes the manner in which some PPP statistics are calculated.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```plaintext
ppp statistics success-sessions { lcp-max-retry | misc-reasons | remote-terminated}

no ppp statistics success-sessions { lcp-max-retry | misc-reasons | remote-terminated}
```

**no**
Disable the specified behavior.

**lcp-max-retry**
Alters statistics calculations so that statistic ppp successful session is the sum of successful sessions and lcp-max-retry.

**misc-reasons**
Alters statistics calculations so that statistic ppp successful session is the sum of successful sessions and misc-reasons.

**remote-terminated**
Alters statistics calculations so that statistic ppp successful session is the sum of successful sessions and remote-terminated.

Usage
Use this command to alter how certain PPP statistics are calculated.

⚠ **Caution:** Use caution when using this command. This command alters the way that some PPP statistics are calculated. Please consult your designated service representative before using this command.

Example
The following command alters the statistic ppp successful session so that it displays the sum of successful sessions and lcp-max-retry:

```plaintext
ppp statistics success-sessions lcp-max-retry
```

The following command disables the alteration of the statistic ppp successful session:
no ppp statistics success-sessions lcp-max-retry
### proxy-dns intercept-list

Enters the HA Proxy DNS Configuration Mode and defines a name of a redirect rules list for the domain name servers associated with a particular FA or group of FAs.

**Important:** HA Proxy DNS Intercept is a license-enabled feature.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
[ no ] proxy-dns intercept-list name
```

- **no**
  
  Removes the intercept list from the system.

- **proxy-dns intercept-list name**
  
  Defines the rules list and enters the Proxy DNS Configuration Mode.

  `name` must be a string from 1 to 63 characters in length.

**Usage**

Use this command to define a name for a list of rules pertaining to the IP addresses associated with the foreign network’s DNS. Up to 128 rules of any type can be configured per rules list.

Upon entering the command, the system switches to the HA Proxy DNS Configuration Mode where the lists can be defines. Up to 64 separate rules lists can be configured in a single AAA context.

This command and the commands in the HA Proxy DNS Configuration Mode provide a solution to the Mobile IP problem that occurs when a MIP subscriber, with a legacy MN or MN that does not support IS-835D, receives a DNS server address from a foreign network that is unreachable from the home network. The following flow shows the steps that occur when this feature is enabled:
By configuring the Proxy DNS feature on the Home Agent, the foreign DNS address is intercepted and replaced with a home DNS address while the call is being handled by the home network.

Example
The following command creates a proxy DNS rules list named `list1` and places the CLI in the HA Proxy DNS Configuration Mode:

```
proxy-dns intercept-list list1
```
radius accounting

Configures the current context’s RADIUS accounting function options.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius accounting { archive [ stop-only ] | deadtime dead_minutes | detect-dead-server { consecutive-failures count | keepalive | response-timeout seconds } | interim interval seconds | max-outstanding msgs | max-pdu-size octets | max-retries | max-transmission-trans | timeout idle_seconds | unestablished-sessions }

no radius accounting { archive | detect-dead-server | interim interval | max-transmissions | unestablished-sessions }

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


no
Removes earlier configuration for the specified keyword.

default
Configures this command with the default settings.

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

stop-only specifies archiving of STOP accounting messages only.

deadtime dead_minutes
Default: 10
Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable. dead_minutes must be an integer from 0 through 65535.

detect-dead-server { consecutive-failures count | keepalive | response-timeout seconds }

consecutive-failures count: Default: 4. Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable. count must be an integer from 0 through 1000.
**keepalive**: Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default is disabled.

**response-timeout seconds**: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state. *seconds* must be an integer from 1 through 65535.

---

**Important**: If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server is considered unreachable, or dead.

---

**interim interval seconds**

Default: Disabled

Specifies the time interval (in seconds) for sending accounting INTERIM-UPDATE records. *seconds* must be an integer from 50 through 4000000.

---

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

---

**max-outstanding msgs**

Default: 256

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

---

**max-pdu-size octets**

Default: 4096

Specifies the maximum sized packet data unit which can be accepted/generated in bytes (octets). *octets* must be an integer from 512 through 4096.

---

**max-retries tries**

Default: 5

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. *tries* must be an integer from 0 through 65535. Once the maximum number of retries is reached this is considered a single failure for the consecutive failures count for detecting dead servers.

---

**max-transmissions trans**

Default: Disabled

Sets the maximum number of transmissions for a RADIUS Accounting message before the message is declared as failed. *trans* must be an integer from 1 through 65535.

---

**timeout seconds**

Default: 3

Specifies the amount of time to wait for a response from a RADIUS server before retransmitting a request. *seconds* must be an integer from 1 through 65535.
unestablished-sessions
Indicates RADIUS STOP events are to be generated for sessions which were initiated but never fully established.

Usage
Manage the RADIUS accounting options according to the RADIUS server used for the context.

Example
The following commands specify accounting options.

```
radius accounting detect-dead-server consecutive-failures 5
radius accounting max-pdu-size 1024
radius accounting timeout 16
```

The following commands disable/clear the options.

```
no radius accounting interim interval 10
no radius accounting unestablished-sessions
```
radius accounting algorithm

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

default radius accounting algorithm

**default**

Configures this command with the default settings.
Default: first-server

**first-n \text{n}**

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

**first-server**

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

**round-robin**

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

Usage

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

Example

The following command specifies to use the round-robin algorithm to select the RADIUS server:
radius accounting algorithm round-robin
radius accounting apn-to-be-included

Configures the APN name to be included for RADIUS accounting.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

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

default radius accounting apn-to-be-included

**Usage**
Use this command to configure the APN name for RADIUS Accounting. This can be set to either gi or gn.

**Example**
The following command specifies the usage of Gn APN name in the RADIUS accounting request:

```
radius accounting apn-to-be-included gn
```
radius accounting billing-version

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius accounting billing-version version

default radius accounting billing-version

default
Configures this command with the default setting.
Default: 0

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

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

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

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

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

Product
GGSN

Privilege
Security Administrator, Administrator

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

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

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

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

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

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

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

default radius accounting gtp trigger-policy
radius accounting ha policy

Configures the RADIUS accounting policy for HA sessions.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

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

**session-start-stop**
Specifies to send Accounting Start when the session is connected, and send Accounting Stop when the session is disconnected. This is the default behavior.

**custom1-aaa-res-mgmt**
Accounting Start/Stop messages are generated to assist special resource management done by AAA servers. It is similar to the session-start-stop accounting policy, except for the following differences:

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

**Usage**
Use this command to set the behavior of the AAA accounting for an HA session.

**Example**
Use the following command to set the HA accounting policy to `custom1-aaa-res-mgmt`:

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

This command configures the volume of uplink and downlink volume octet counts that triggers RADIUS interim accounting.

**Product**
GGSN, PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
radius accounting interim volume { downlink bytes uplink bytes | total bytes | uplink bytes downlink bytes }

no radius accounting interim volume
```

- **no**
  Disables volume based RADIUS accounting.

- **downlink bytes uplink bytes**
  Specifies the downlink to uplink volume limit for RADIUS Interim accounting, in bytes. 
  `bytes` must be an integer from 100000 through 4000000000.

- **total bytes**
  Specifies the total volume limit for RADIUS interim accounting in bytes. 
  `bytes` must be an integer from 100000 through 4000000000.

- **uplink bytes downlink bytes**
  Specifies the uplink to downlink volume limit for RADIUS interim accounting in bytes. 
  `bytes` must be an integer from 100000 through 4000000000.

**Usage**

Use this command to trigger RADIUS interim accounting based on the volume of uplink and downlink bytes.

**Example**

The following command triggers RADIUS interim accounting when the total volume of uplink and downlink bytes reaches 110000:

```
radius accounting interim volume total 110000
```
radius accounting ip remote-address

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

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

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

no
Removes earlier configuration for the specified keyword.

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

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

Usage
This command is used as part of the Remote Address-based Accounting feature to both configure remote IP address lists and enable the collection of accounting data for the addresses in those lists on a per-subscriber basis.
Individual subscriber can be associated to remote IP address lists through the configuration/specification of an attribute in their local or RADIUS profile. (Refer to the radius accounting command in the Subscriber Configuration mode.) When configured/specified, accounting data is collected pertaining to the subscriber’s communication with any of the remote addresses specified in the list.
Once this functionality is configured on the system and in the subscriber profiles, it must be enabled by executing this command with the collection keyword.

Example

radius accounting ip remote-address collection
**radius accounting keepalive**

Configures the keepalive authentication parameters for the RADIUS accounting server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

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

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

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

**no**
Removes configuration for the specified keyword.

**default**
Configures this command with the default settings.

**calling-station-id id**
Configures the Calling-Station-Id to be used for the keepalive authentication.
`id` must be an alpha and/or numeric string of 1 through 15 characters in length.
Default: 0000000000000

**consecutive-response number**
Configures the number of consecutive authentication response after which the server is marked as reachable.
`number` must be an integer from 1 through 5.
Default: 1

**framed-ip-address ip_address**
Configures the framed-ip-address to be used for the keepalive accounting.
`ip_address` must be specified using the standard IPv4 dotted decimal notation.

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

**retries number**
Configures the number of times the keepalive access request to be sent before marking the server as unreachable.
radius accounting keepalive

number must be an integer from 3 through 10.
Default: 3

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

username name
Configures the username to be used for the authentication.
name must be an alpha and/or numeric string of 1 through 127 characters in length.
Default: Test-Username

Usage
Configures the keepalive authentication parameters for the RADIUS accounting server.

Example
The following command sets the username for the radius keepalive access requests:

    radius accounting keepalive username Test-Username2

The following command sets the number of retries to 4.

    radius accounting keepalive retries 4
radius accounting rp

Configures the current context’s RADIUS accounting R-P originated call options.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

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

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

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

---

**no**

Removes earlier configuration for the specified keyword.

---

**default**

Configures this command with the default settings.

---

**handoff-stop { immediate | wait-active-stop }**

**Default:** `wait-active-stop`

Specifies the behavior of generating accounting STOP when handoff occurs.

- **immediate**: Indicates that accounting STOP should be generated immediately on handoff, i.e. not to wait active-stop from the old PCF.

- **wait-active-stop**: Indicates that accounting STOP is generated only when active-stop received from the old PCF when handoff occurs.

---

**tod minute hour**

Specifies the time of day a RADIUS event is to be generated for accounting. Up to four different times of the day may be specified through separate commands.

- `minute` must be an integer from 0 through 59.
- `hour` must be an integer from 0 through 23.

---

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

**Default:** `active-handoff`: Disabled

- `active-handoff`: Enabled
- `active-stop`: Disabled

Configures the events for which a RADIUS event is generated for accounting as one of the following:
**active-handoff**: Disables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Instead, two R-P events occur (one for the Connection Setup, and the second for the Active-Start).

**active-start-param-change**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

**active-stop**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

---

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

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

Default: **airlink-usage**: Disabled

**custom**:

- **active-handoff** = Disabled
- **active-start-param-change** = Disabled
- **active-stop** = Disabled
- **standard** = Enabled

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

- **airlink-usage [ counter-rollover ]**: Designates the use of Airlink-Usage RADIUS accounting policy for R-P, which generates a start on Active-Starts, and a stop on Active-Stops.

If the **counter-rollover** option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than \((2^{32} - 1)\) in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than \(2^{32}\) thus ensuring the accuracy of the count. The system, may, at its discretion, send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped. Note that a STOP/START pair is never generated unless the subscriber RP session is in the Active state, since octet/packet counts are not accumulated when in the Dormant state.

- **custom**: Specifies the use of custom RADIUS accounting policy for R-P. The custom policy can consist of the following:

  - **active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start).

  - **active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

---

**Important**: Note that a custom trigger policy with only **active-start-param-change** enabled is identical to the **standard** trigger-policy.

- **active-stop**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

---

**Important**: If the **radius accounting rp trigger-policy custom** command is executed without any of the optional keywords, all custom options are disabled.
**standard**: Specifies the use of Standard RADIUS accounting policy for R-P in accordance with IS-835B.

**trigger-stop-start**

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

**Usage**

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

**Example**

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

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

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

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

Configures RADIUS accounting server(s) in the current context for accounting.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

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

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

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

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

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

- **ip_address**
  Specifies the IP address of the accounting server. `ip_address` must be specified in dotted decimal notation for IPv4 or colon notation for IPv6. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

- **[ encrypted ] key value**
  Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted. The key `value` must be a string of 1 to 15 alpha and/or numeric characters or a string of 1 to 30 alpha and/or numeric characters when encrypted.
  The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `key` keyword is the encrypted version of the plaint text key. Only the encrypted key is saved as part of the configuration file.

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

**acct-off { enable | disable }

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

**max msgs

Default: 0
Specifies the maximum number of outstanding messages that may be allowed to the server. *msgs* must be an integer from 1 through 256.

**oldports

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

**port port_number

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

**priority priority

Default: 1000
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to. *priority* must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the `-noconfirm` option, you are not asked for confirmation and multiple servers could be assigned the same priority.

**type { mediation-device | standard }

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

**admin-status { enable | disable }

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

**-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.
Usage

This command is used to configure the RADIUS accounting servers with which the system is to communicate for accounting. Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

```
radius accounting server 1.2.3.4 key sharedKey port 1024 max 127
radius accounting server 1.2.5.6 encrypted key scrambledKey oldports priority10
no radius accounting server 1.2.5.6
```

Following command sets the accounting server with mediation device transaction for AAA server 1.2.4.6:

```
radius mediation-device accounting server 1.2.3.4 key sharedKey port 1024 max 127
```
radius algorithm

Configures the RADIUS authentication server selection algorithm for the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius algorithm { first-server | round-robin }

default radius algorithm

default
Configures this command with the default settings.

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

Usage
Set the context’s RADIUS server selection algorithm to ensuring proper load distribution through the servers available.

Example

radius algorithm first-server
radius algorithm round-robin
radius allow

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

**no**
Removes earlier configuration for the specified keyword.

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

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

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

**Example**

```bash
radius allow authentication-down
no radius allow authentication-down
radius allow accounting-down
no radius allow accounting-down
```
radius attribute

Configures the system’s RADIUS identification parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
radius attribute { nas-identifier id | nas-ip-address address primary_address [ backupsecond_address ] [ nexthop-forwarding-address nexthop_address ] [ vlan vlan_id ] [ mpls-label input in_label_value output out_label_value1 out_label_value2 ] }
```

```
no radius attribute { nas-identifier | nas-ip-address }
```

```
default radius attribute nas-identifier
```

```
no
```
Removes earlier configuration for the specified keyword.

```
default
```
Configures this command with the default settings.

```
nas-identifier id
```
Specifies the attribute name by which the system will be identified in Access-Request messages. *id* must be a case-sensitive alpha and/or numeric string of 1 through 32 characters in length.

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

`primary_address`: The IP address of the primary interface to use in the current context. This must be specified in dotted decimal notation for IPv4 or colon notation for IPv6.

```
backup second_address
```
Specifies the IP address of the secondary interface to use in the current context. This must be in dotted decimal notation for IPv4 or colon notation for IPv6.

```
mls-label input in_label_value | output out_label_value1 [ out_label_value2 ]
```
This command configures the traffic from the specified AAA client NAS IP address to use the specified MPLS labels.

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

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

`next-hop-forwarding-address` `next-hop_address`

Configures the next hop IP address for this NAS IP address.
`next-hop_address` must be an IPv4 address or an IPv6 address in standard format.

`vlan` `vlan_id`

Configures VLAN ID to be associated with the next-hop IP address.
`vlan_id` must be an integer from 1 through 4094.

**Usage**

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

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

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

• All current in-process RADIUS authentication messages from the entire system are cancelled. The authentication message is re-sent, with retries preserved, using the new active `nas-ip-address`. The value of Event-Timestamp is preserved.

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

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

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

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

**Example**

```
radius attribute nas-ip-address 1.2.3.4

no radius attribute nas-identifier sampleID
```
**radius authenticate**

Enables (allows) and disables (prevents) the authentication of user names that are blank or empty. This is enabled by default.

**Product**  
PDSN

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
[ no | default ] radius authenticate null-username
```

- **default**  
  Configures this command with the default settings for authenticating, sending Access-Request messages to the AAA server, all user names, including NULL user names.

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

**Usage**

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

**Example**

To disable sending Access-Request messages for user names (NAI) that are blank, enter the following command:

```
no radius authenticate null-username
```

To re-enable sending Access-Request messages for user names (NAI) that are blank, enter the following command:

```
radius authenticate null-username
```
radius authenticate apn-to-be-included

Configures the APN name to be included for RADIUS authentication.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default ] radius authenticate apn-to-be-included { gi | gn }
```

- **default**
  Configures this command with the default settings.

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

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

**Usage**

Use this command to configure the APN name for RADIUS authentication. This can be set to either gi or gn.

**Example**

The following command specifies the usage of Gn APN name in the RADIUS authentication request.

```
radius authenticate apn-to-be-included gn
```
radius authenticator-validation

Enables (allows) and disables (prevents) the MD5 authentication of RADIUS user. This is enabled by default.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no | default ] radius authenticator-validation
```

- **no**
  
  Disables MD5 authentication validation for an Access-Request message to the AAA server.

- **default**

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

- **no**

  Disable sending an Access-Request message to the AAA server for usernames (NAI) that are blank.

**Usage**

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

**Example**

To disable MD5 authentication validation for Access-Request messages for usernames (NAI), enter the following command:

```
no radius authenticator-validation
```

To enable MD5 authentication validation for Access-Request messages for usernames (NAI), enter the following command:

```
radius authenticator-validation
```
radius change-authorize-nas-ip

Defines the NAS IP address and UDP port on which the current context will listen for Change of Authorization (COA) messages and Disconnect Messages (DM). If the NAS IP address is not defined with this command, any COA or DM messages from the RADIUS server are returned with a Destination Unreachable error.

Product
PDSN, FA, HA, GGSN, LNS

Privilege
Security Administrator, Administrator

Syntax

[ no ] radius change-authorize-nas-ip ip_address [ encrypted ] key value [ port port ] [ event-timestamp-window window ] [ no-nas-identification-check] [ no-reverse-path-forward-check ] [ mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ] ]

no

Deletes the NAS IP address information which disables the system from receiving and responding to COA and DM messages from the RADIUS server.

ip_address

Specifies the NAS IP address of the current context’s AAA interface that was defined with the radius attribute command.

ip_Address can either be an IPv4 address expressed in dotted decimal notation, or an IPv6 address expressed in colon notation.

[ encrypted ] key value

Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted. The key value must be a string of 1 to 15 alpha and/or numeric characters or a string of 1 to 30 alpha and/or numeric characters when encrypted.

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

port port

Default: 3799

The UDP port on which to listen for COA and DM messages.

event-timestamp-window window

Default: 300 seconds

window must be an integer from 0 through 4294967295.

When a COA or DM request is received with an event-time-stamp, if the current-time is greater than received-pkt-event-time-stamp plus event-time-stamp-window, the packet is silently discarded.

When a COA or DM request is received without the event-timestamp attribute, the packet is silently discarded.
If `window` is specified as 0 (zero), this feature is disabled; the event-time-stamp attribute in COA or DM messages is ignored and the event-time-stamp attribute is not included in NAK or ACK messages.

**no-nas-identification-check**
Disables the context from checking the NAS Identifier/ NAS IP Address while receiving the CoA/DM requests.
By default this check is enabled.

**no-reverse-path-forward-check**
Disables the context from checking whether received COA or DM packets are from one of the AAA servers configured in the current context. Only the src-ip address in the received COA or DM request is validated and the port and key are ignored.
reverse-path-forward-check is enabled by default.
When reverse-path-forward-check is disabled, CoA and DM messages are accepted from any AAA server.

**mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ]**
This command configures COA traffic to use the specified MPLS labels.
- `in_label_value` is the MPLS label that identifies inbound COA traffic.
- `out_label_value1` & `out_label_value2` identify the MPLS labels to be added to COA response.
- `out_label_value1` is the inner output label.
- `out_label_value2` is the outer output label.
MPLS label values must be an integer from 16 to 1048575.

**Usage**
Use this command to enable the current context to listen for COA and DM messages.
Any one of the following RADIUS attributes may be used to identify the subscriber:
- **3GPP-IMSI**: The IMSI of the subscriber. It may include the 3GPP-NSAPI attribute to delete a single PDP context rather than all of the PDP contexts of the subscriber when used with the GGSN product.
- **Framed-IP-address**: The IP address of the subscriber.
- **Acct-Session-Id**: Identifies a subscriber session or PDP context;

**Important**: For the GGSN product, the value for Acct-Session-Id that is mandated by 3GPP is used instead of the special value for Acct-Session-Id that we use in the RADIUS messages we exchange with a RADIUS accounting server.

**Important**: When this command is used in conjunction with the GGSN, CoA functionality is not supported.

**Example**
Specify the IP address 192.168.100.10 as the NAS IP address, a key value of 123456 and use the default port of 3799, by entering the following command:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456
```
Following disables the nas-identification-check for the above parameters:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456 no-nas-identification-check
```
radius charging

Configures basic RADIUS options for Active Charging Services.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | default ] radius charging {
  daytime dead_minutes
  detect-dead-server { 
    consecutive-failures count | response-timeout seconds }
  max-outstanding msgs 
  max-retries tries 
  max-transmissions transmissions | timeout idle_seconds }
```

---

**no**

Removes configuration for the specified keyword.

---

**default**

Configures this command with the default settings.

---

**daytime dead_minutes**

Default: 10

Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable. `dead_minutes` must be an integer from 0 through 65535.

---

**detect-dead-server { consecutive-failures count | response-timeout seconds }**

**consecutive-failures count**: Default: 4. Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable. `count` must be an integer from 0 through 1000.

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

---

**max-outstanding msgs**

Default: 256

Specifies the maximum number of outstanding messages a single AAA manager instance will queue. `msgs` must be an integer from 1 through 4000.

---

**max-retries tries**

Default: 5

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. `tries` must be an integer from 0 through 65535.

---

**max-transmissions transmissions**

Default: Disabled
Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with the `max-retries` for each server. When failing to communicate with a RADIUS server, the subscriber is failed once all of the configured RADIUS servers have been exhausted or once the configured number of maximum transmissions is reached. For example, if 3 servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried 4 times (once plus 3 retries), the secondary server is tried 4 times, and then a third server is tried 4 times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

`transmissions` must be an integer from 1 through 65535.

**timeout idle_seconds**

Default: 3

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

**Usage**

Manage the basic Charging Service RADIUS options according to the RADIUS server used for the context.

**Example**

```
radius charging detect-dead-server consecutive-failures 6
radius charging timeout 300
```
radius charging accounting algorithm

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

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

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

**first-n n**
Default: 1 (Disabled)
Specifies that the AGW must send accounting data to n (more than one) AAA servers based on their priority. Response from any one of the n AAA servers would suffice to proceed with the call. The full set of accounting data is sent to each of the n AAA servers.

n is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128.

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

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

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

Example
The following command specifies to use the round-robin algorithm to select the RADIUS server:

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

Configures RADIUS charging accounting servers in the current context for Active Charging Services prepaid accounting.

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

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

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

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

- [ encrypted ] key value
  Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted. The key value must be a string of 1 to 15 alpha and/or numeric characters, or when encrypted a string of 1 to 30 alpha and/or numeric characters.
  The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the keyword is the encrypted version of the plaintext key. Only the encrypted key is saved as part of the configuration file.

- max msgs
  Default: 0
  Specifies the maximum number of outstanding messages that may be allowed to the server.
  msgs must be integer from 0 through 4000.

- max-rate max_rate
  Default: Disabled
  Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server.
  max_rate must be an integer from 1 through 1000.
oldports
Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

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

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

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

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
This command is used to configure the RADIUS charging accounting server(s) with which the system is to communicate for Active Charging Services prepaid accounting requests.

Example
Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

radius charging accounting server 1.2.3.4 key sharedKey port 1024 max 127
radius charging accounting server 1.2.5.6 encrypted key scrambledKey oldports priority:10 ]
no radius charging accounting server 1.2.5.6
radius charging algorithm

Configures the RADIUS authentication server selection algorithm for Active Charging Services for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

default radius charging algorithm

default

Configures this command with the default settings.
Default: first-server

first-server

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

round-robin

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

Usage

Set the context’s RADIUS server selection algorithm for Active Charging Services to ensure proper load distribution through the servers available.

Example

radius algorithm first-server
radius algorithm round-robin
**radius charging server**

Configures the RADIUS charging server(s) in the current context for Active Charging Services prepaid authentication.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

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

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

**no**

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

**ip_address**

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

**[ encrypted ] key value**

Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted. The `key` value must be a string of 1 to 15 alpha and/or numeric characters, or when encrypted a string of 1 to 30 alpha and/or numeric characters. The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `key` keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

**max msgs**

Default: 256

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

**max-rate max_rate**

Default: Disabled

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. `max_rate` must be an integer from 1 through 1000.

**oldports**

Sets the UDP communication port to the old default for RADIUS communications to 1645.
Context Configuration Mode Commands

**radius charging server**

Default: 1812
Specifies the port number to use for communications. `port_number` must be an integer from 0 through 65535.

**priority priority**

Default: 1000
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to. `priority` must be a value in the range 1 through 1000 where 1 is the highest priority.

**admin-status { enable | disable }**

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

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

This command is used to configure the RADIUS charging server(s) with which the system is to communicate for Active Charging Services prepaid authentication requests.

**Example**

Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

```sh
radius charging server 1.2.3.4 key sharedKey port 1024 max 127
radius charging server 1.2.5.6 encrypted key scrambledKey oldports priority 10
no radius server 1.2.5.6
```
radius dictionary

This command configures the RADIUS dictionary for RADIUS prepaid charging.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius dictionary dictionary

default radius dictionary

default
Configures this command with the default setting.

dictionary dictionary
Specifies the dictionary to use.
The possible values are described in the following table.

Table 17.

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in 3GPP 32.015.</td>
</tr>
<tr>
<td>3gpp2</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>customXXX</td>
<td>These are customized dictionaries. For information on custom dictionaries, please contact your local service representative. XX is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all the attributes in the starent-vas1 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
</tbody>
</table>

Important: RADIUS dictionary custom23 should be used in conjunction with Active Charging Service (ACS). Refer to the Enhanced Charging Service Configuration and Reference Guide for more information.
radius dictionary

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

Usage

Use this command to assign the RADIUS dictionary according to the RADIUS server used for the context.

Example

The following command sets custom23 as dictionary for prepaid charging:

```
radius dictionary custom23
```
radius group

This command has been deprecated and is replaced by AAA Server Group configurations. See the AAA Server Group Configuration Mode Commands chapter.
radius ip vrf

This command associates the default AAA group with a Virtual Routing and Forwarding (VRF) Context instance for GRE tunnel interface configuration. By default the VRF is NULL, which means that default AAA group is associated with global routing table.

Product
All

Privilege
Security Administrator, Administrator

Syntax

radius ip vrf vrf_name
no radius ip vrf

Example
Following command associates VRF context instance GRE_vrf1 with this AAA group:

radius ip vrf GRE_vrf1
radius keepalive

Configures the keepalive authentication parameters for the RADIUS server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

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

default
Configures this command with the default settings.

calling-station-id id
Configures the Calling-Station-Id to be used for the keepalive authentication. id must be an alpha and/or numeric string of 1 through 15 characters in length.
Default: 000000000000000

consecutive-response number
Configures the number of consecutive authentication response after which the server is marked as reachable. number must be integer from 1 through 5.
Default: 1

encrypted password
Designates use of encryption for the password. password must be an alpha and/or numeric string of 1 through 64 characters in length.
Default: Test-Password

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

password
Configures the password to be used for the authentication. password must be an alpha and/or numeric string of 1 through 64 characters in length.
Default: Test-Password

retries number
Configures the number of times the keepalive access request to be sent before marking the server as unreachable. number must be an integer from 3 through 10.
Default: 3
timeout seconds
Configures the time interval between each keepalive access request retries. seconds must be an integer from 1 through 30.
Default: 3 seconds

username name
Configures the username to be used for the authentication. name must be an alpha and/or numeric string of 1 through 127 characters in length.
Default: Test-Username

valid-response access-accept [ access-reject ]
Configures the valid response for the authentication request.
If access-reject is configured, then both access-accept and access-reject are considered as success for the keepalive authentication request.
If access-reject is not configured, then only access-accept is considered as success for the keepalive access request.
Default: keepalive valid-response access-accept

Usage
Configures the keepalive authentication parameters for the RADIUS server.

Example
The following command sets the user name for the RADIUS keepalive access requests:

    radius keepalive username Test-Username2

The following command sets the number of retries to 4.

    radius keepalive retries 4
radius mediation-device

See the `radius accounting server` command.
radius probe-interval

Configures the interval duration between two RADIUS authentication probes.

Product
GGSN, HA

Privilege
Security Administrator, Administrator

Syntax

radius probe-interval seconds

default radius probe-interval

default
Configures this command with the default settings.

seconds
Default: 3
Specifies the amount of time in seconds to wait before sending another probe authentication request to a RADIUS server. seconds must be an integer from 1 through 65535.

Usage
Use this command for Home Agent Geographical Redundancy (HAGR) support to set the duration between two authentication probes to the RADIUS server.

Example
Following command sets the authentication probe interval to 30 seconds.

radius probe-interval 30
radius probe-max-retries

Configures the number of retries for RADIUS authentication probe response.

**Product**
GGSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

radius probe-max-retries retries

default radius probe-max-retries

default

Configures this command with the default settings.

retries

Default: 5

Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed.

retries must be an integer from 1 through 65535.

**Usage**

Use this command for Interchassis Session Recovery (ICSR) support to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

**Example**
The following command sets the maximum number of retries to 6:

radius probe-max-retries 6
radius probe-timeout

Configures the timeout duration to wait for a response for RADIUS authentication probes.

Product
GGSN, HA

Privilege
Security Administrator, Administrator

Syntax

radius probe-timeout idle_seconds

default radius probe-timeout

default
Configures this command with the default settings.

idle_seconds
Default: 3
Specifies the number of seconds to wait for response from the RADIUS server before resending the authentication probe.
idle_seconds must be an integer from 1 through 65535.

Usage
Use this command for Interchassis Session Recovery (ICSR) support to set the duration to wait for response before re-sending the RADIUS authentication probe to the RADIUS server.

Example
The following command sets the authentication probe timeout to 120 seconds:
radius probe-timeout 120
**radius server**

Configures RADIUS authentication server(s) in the current context for authentication.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
radius server ip_address [ encrypted ] key value [ max msgs ] [ max-rate
max_rate ] [ oldports ] [ port port_number ] [ priority priority ] [ probe | no-
probe ] [ probe-username user_name ] [ probe-password [ encrypted ] password
password ] [ type { mediation-device | standard } ] [ admin-status { enable |
disable } ] [ -noconfirm ]
```

**no radius server ip_address [ oldports ] [ port port_number ]**

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

**ip_address**
Specifies the IP address of the server. `ip_address` must be specified in dotted decimal notation for IPv4 or colon notation for IPv6. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

**[ encrypted ] key value**
Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted. The `key value` must be a string of 1 to 15 alpha and/or numeric characters or a string of 1 to 30 alpha and/or numeric characters when encrypted. The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `key` keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

**max msgs**
Default: 256
Specifies the maximum number of outstanding messages that may be allowed to the server.
`msgs` must be an integer from 0 through 4000.

**max-rate max_rate**
Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server.
`max_rate` must be an integer from 1 through 1000.
Default: disabled
oldports
Sets the UDP communication port to the old default for RADIUS communications to 1645.

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

priority priority
Default: 1000
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to. priority must be a value in the range 1 through 1000 where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the -noconfirm option, you are not asked for confirmation and multiple servers could be assigned the same priority.

probe
Enable probe messages to be sent to the specified RADIUS server.

no-probe
Disable probe messages from being sent to the specified RADIUS server. This is the default behavior.

probe-username username
The user name sent to the RADIUS server to authenticate probe messages. user_name must be an alpha and/or numeric string of 1 through 127 characters in length.

probe-password [ encrypted ] password  password
The password sent to the RADIUS server to authenticate probe messages.
encrypted: This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
password: Specifies the probe-user password for authentication. password must be an alpha and/or numeric string of 1 through 63 characters in length.

type { mediation-device | standard }
Specifies the type of transactions the RADIUS server accepts.
mediation-device: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local sales representative for licensing information.
standard: Specifies standard AAA transactions. (Default)

admin-status { enable | disable }
Enables or disables the RADIUS { authentication | accounting | charging } server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.
-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
This command is used to configure the RADIUS authentication server(s) with which the system is to communicate for authentication.
Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example
radius server 1.2.3.4 key sharedKey port 1024 max 127
radius server 1.2.5.6 encrypted key scrambledKey oldports priority 10
no radius server 1.2.5.6
route-access-list extended

This command configures an access list for filtering routes based on a specified range of IP addresses.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
route-access-list extended identifier { deny | permit } ip { network_parameter } { mask_parameter }
```

```
no route-access-list extended identifier { deny | permit } ip { network_parameter } { mask_parameter }
```

- **no**
  Deletes the specified route access list.

  **identifier**
  A value to identify the route access list. `identifier` must be an integer from 100 through 999.

  **deny**
  Deny routes that match the specified criteria.

  **permit**
  Permit routes that match the specified criteria.

  **network_parameter**
  This specifies the network portion of the route to match. The network portion of the route is mandatory and must be expressed in one of the following ways:
  - `ip_address wildcard_mask`: A network address and wildcard mask expressed in IPv4 dotted decimal notation. `(192.168.100.0 0.0.0.255)`
  - `any`: Match any network address.
  - `host network_address`: Match the specified network address exactly. `network_address` must be an IPv4 address specified in dotted decimal notation.

  **mask_parameter**
  This specifies the mask portion of the route to match. The mask portion of the route is mandatory and must be expressed in one of the following ways:
  - `mask_address wildcard_mask`: A mask address and wildcard mask expressed in IPv4 dotted decimal notation. `(255.255.255.0 0.0.0.255)`
  - `any`: Match any network mask.
  - `host mask_address`: Match the specified mask address exactly. `mask_address` must be an IPv4 address specified in dotted decimal notation.
Usage
Use this command to create an extended route-access-list that matches routes based on network addresses and masks.

Example
Use the following command to create an extended route-access-list:

```
route-access-list extended 100 permit ip 192.168.100.0 0.0.0.255 255.255.255.0 0.0.0.255
```
route-access-list named

This command configures an access list for filtering routes based on a network address and net mask.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
route-access-list named list_name { deny | permit } { ip_address/mask | any } [ exact-match ]
```

```
no route-access-list named list_name { deny | permit } { ip_address/mask | any } [ exact-match ]
```

- **no**
  Deletes the specified route access list.

- **list_name**
  A name that identifies the route access list. `list_name` must be a string of 1 through 79 alphanumeric characters in length.

- **deny**
  Deny routes that match the specified criteria.

- **permit**
  Permit routes that match the specified criteria.

- **ip_address/mask**
  The IP address (in dotted-decimal notation) and the number of subnet bits, representing the subnet mask in shorthand. This variable must be entered in the dotted-decimal notation/subnet bits format (1.1.1.1/24).

- **any**
  Match any route.

- **exact-match**
  Match the IP address prefix exactly.

**Usage**

Use this command to create route-access lists that specify routes that are accepted.

**Example**

---

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01
Use the following command to create a route access list named list27 that permits routes that match 192.168.1.0/24 exactly:

```
route-access-list named list27 permit 192.168.1.0/24 exact-match
```

To delete the list, use the following command:

```
no route-access-list named list27 permit 192.168.1.0/24 exact-match
```
route-access-list standard

This command configures an access-list for filtering routes based on network addresses.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

route-access-list standard identifier { permit | deny } { ip_address wildcard mask | any | host network_address }

no route-access-list standard identifier { permit | deny } { ip_address wildcard mask | any | host network_address }

no
Deletes the specified route access list.

identifier
This is a value that identifies the route-access-list. This must be an integer from 1 through 99.

deny
Deny routes that match the specified criteria.

permit
Permit routes that match the specified criteria.

ip_address wildcard mask
The IP address and subnet mask to match for routes. Both ip_address and wildcard mask must be entered in IPv4 dotted decimal notation. (192.168.100.0 255.255.255.0)

any
Match any route.

host network_address
Routes must match the specified network address as if it had a 32-bit network mask. network_address must be an IPv4 address specified in dotted decimal notation.

Usage
Use this command to create route-access-lists that specify routes that are accepted.

Example
Use the following command to create a route access list with an identifier of 10 that permits routes:

```
route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```

To delete the list, use the following command:

```
no route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```
route-map

This command creates a route-map that is used by the routing features and enters Route-map Configuration mode. A route-map allows redistribution of routes. A routemap has a list of match and set commands associated with it. The match commands specify the conditions under which redistribution is allowed and the set commands specify the particular redistribution actions to be performed if the criteria specified by match commands are met. Route-maps are used for detailed control over route distribution between routing processes. Up to eight route-maps can be created in each context. Refer to the Route-map Configuration mode commands for more information.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
route-map map_name { deny | permit } seq_number
no route-map map_name
```

```
no

Deletes the specified route-map.
```

```
map_name

The name of the route-map to create or edit. This is a string of characters from 1 through 69 characters long.
```

```
deny

If the deny parameter is specified and the match command criteria are met, the route is not redistributed and any other route maps with the same map name are not examined. Set commands have no affect on deny route-maps.
```

```
permit

If the permit parameter is specified, and the match criteria are met, the route is redistributed as specified by set actions. If the match criteria are not met, the next route map with the same name is tested.
```

```
seq_number

The sequence number that indicates the position a new route map is to have in the list of route maps already configured with the same name. Route maps with the same name are tested in ascending order of their sequence numbers. This must be an integer from 1 through 65535.
```

Usage

Use this command to create route maps that allow redistribution of routes based on specified criteria and set parameters for the routes that get redistributed. The chassis supports a maximum of 64 route maps per context.
Example
To create a route map named map1 that permits routes that match the specified criteria, use the following command:

```
route-map map1 permit 10
```

To delete the route-map, enter the following command:

```
no route-map map1 permit 10
```
**router**

This command enables the OSPF routing functionality and enters the OSPF Configuration mode. Refer to the OSPF Configuration Mode Commands chapter for details on OSPF Configuration mode commands.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
router {ospf | bgp as_number}

no router {ospf | bgp as_number}
```

- **no**
  Disables the specified routing support in the current context.

- **ospf**
  Enable OSPF routing in this context and enter OSPF Configuration mode.

- **bgp as_number**
  Enable a BGP routing service for this context and assign it the specified AS number.\( as\_number \text{ must be an integer from 1 through 65535.} \)

**Important:** BGP routing is supported only for use with the HA.

**Usage**

Use this command to enable and configure OSPF and BGP routing in the current context.

**Important:** You must obtain and install a valid OSPF or BGP-4 feature use license key to use OSPF and BGP routing features. Refer to the System Administration and Configuration Guide for details on obtaining and installing feature use license keys.

**Example**

The following command enables the OSPF routing functionality and enters the OSPF Configuration mode:

```plaintext
router ospf
```

The following command enables a BGP routing service with an AS number of 100, and enters the BGP configuration mode:

```plaintext
router bgp 100
```
server

Configures remote server access protocols for the current context. This command is used to enter the specified protocols configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
server { ftpd | named | sshd | telnetd | tftp }
no server { ftpd | named | sshd | telnetd | tftp } [ kill ]
```

- **no**
  Disables the specified service.

- **ftpd**
  Enters the ftpd server configuration mode.

**Important:** The FTPD server can only be configured in the local context.

- **named**
  Starts the named server.

- **sshd**
  Enters the sshd server configuration mode.

**Important:** The SSH server allows only three unsuccessful login attempts before closing a login session attempt.

- **telnetd**
  Enters the telnetd server configuration mode.

**Important:** The TELNET server allows only three unsuccessful login attempts before closing a login session attempt.

- **tftp**
  Enters the tftp server configuration mode.

**Important:** The TFTPDD server can only be configured in the local context.
kill

Indicates all instances of the server are to be stopped.
This option only works with the ftpd, sshd, telnetd, and tftp commands.

Usage

Enter the context configuration mode for the appropriate, previously defined context, to set the server option(s). Repeat the command as needed to enable/disable more than one option server daemon.

Example

server ftpd
server named
no server tftp
server sshd
server telnetd
no server telnetd kill
service-redundancy-protocol

Configures Interchassis Session Redundancy services for the current context. This command is used to enter the service redundancy protocol configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
service-redundancy-protocol
```

**Usage**
Enter the configuration mode to set the service redundancy protocol options.

**Example**
The following command enters service redundancy protocol mode.

```
service-redundancy-protocol
```
sgw-service

Creates an S-GW service or specifies an existing S-GW service and enters the S-GW service configuration mode for the current context.

Product
S-GW

Privilege
Administrator

Syntax

sgw-service service_name [ -noconfirm ]

no sgw-service service_name

service_name
Specifies the name of the S-GW service. If service_name does not refer to an existing service, the new service is created if resources allow.

no sgw-service service_name
Removes the specified S-GW service from the context.

Usage
Enter the S-GW service configuration mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example
The following command enters the existing S-GW service configuration mode (or creates it if it doesn’t already exist) for the service named sgw-service1:
sgw-service sgw-service1

The following command will remove sgw-service1 from the system:

no sgw-service sgw-service1
sgsn-service

This command creates an SGSN service instance and enters the SGSN Service Configuration Mode. This mode configures or edits the configuration for an SGSN service which controls the SGSN functionality.

An SGSN mediates access to GPRS/UMTS network resources on behalf of user equipment (UE) and implements the packet scheduling policy between different QoS classes. It is responsible for establishing the packet data protocol (PDP) context with the GGSN.

**Important:** For details about the commands and parameters, check the SGSN Service Configuration Mode chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sgsn-service srvc_name
no sgsn-service srvc_name
```

- **no**
  Remove the configuration for the specified SGSN service from the configuration of the current context.

- **srvc_name**
  A unique string of 1 to 63 alphanumeric characters that identify the specific SGSN service.

**Usage**

Use this command to create, edit, or remove an SGSN service.

**Example**

The following command creates an SGSN service named sgsn1 in the current context:

```
sgsn-service sgsn1
```

The following command removes the sgsn service named sgsn1 from the configuration for the current context:

```
no sgsn-service sgsn1
```
sgtp-service

This command creates an SGTP service instance and enters the SGTP Service Configuration Mode. This mode configures the GPRS Tunneling Protocol (GTP) related settings required by the SGSN to support GTP-C (control plane) messaging and GTP-U (user data plane) messaging.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sgtp-service svc_name

no sgtp-service svc_name
```

**no**
Remove the configuration for the specified SGTP service from the configuration of the current context.

```
svc_name
```
A unique string of 1 to 63 alphanumeric characters that identify the specific SGTP service.

**Usage**
Use this command to create, edit, or remove an SGTP service.

**Example**
The following command creates an SGTP service named *sgtp1* in the current context:

```
sgtp-service sgtp1
```

The following command removes the sgsn service named *sgtp1* from the configuration for the current context:

```
no sgtp-service sgtp1
```
ssh

Generates public and private keys for use with the configured SSH server for the current context and sets the public/private key pair to specified values.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ssh { generate key | key data length octets } [ type { v1-rsa | v2-rsa | v2-dsa } ]

no ssh key [ type { v1-rsa | v2-rsa | v2-dsa } ]
```

This command clears configured SSH keys. If type is not specified, all SSH keys are cleared.

**generate key**
This command generates a public/private key pair which is to be used by the SSH server. The generated key pair is in use until the command is issued again.

```plaintext
key data length octets
```

This command sets the public/private key pair to be used by the system where `data` is the encrypted key and `length` is the length of the encrypted key in octets. `data` must be an alpha and/or numeric string of 1 to 1023 characters and `octets` must be a value in the range of 0 through 65535.

```plaintext
[ type { v1-rsa | v2-rsa | v2-dsa } ]
```

Specifies the type of SSH key to generate. If type is not specified, all three key types are generated.

- **v1-rsa**: SSH v1 RSA host key only
- **v2-rsa**: SSH v2 DSA host key only
- **v2-dsa**: SSH v2 RSA host key only

**Important**: For maximum security, it is recommended that only SSH v2 be used. **v2-rsa** is the recommended key type.

**Usage**
Generate secure shell keys for use in public key authentication.

**Example**

```plaintext
ssh generate key

ssh key g6j93fw59cx length 128
```
subscriber

Configures the specified subscriber for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
subscriber { default | name user_name }

no subscriber { default | name user_name }
```

- **no**
  Indicates the subscriber specified is to be removed from the list of allowed users for the current context.

- **default | name user_name**
  - **default**: enters the subscriber configuration mode for the context’s default subscriber settings.
  - **name user_name**: specifies the user which is to be allowed to use the services of the current context.
  user_name must be from 1 to 127 alpha and/or numeric characters.

**Usage**
Enter the subscriber configuration mode for actual users as well as for a default subscriber for the current context.

**Important**: A maximum of 128 subscribers and/or administrative users may be locally configured per context.

**Example**

```plaintext
subscriber default

no subscriber default

subscriber name user1

no subscriber name user1
```
threshold

The commands in this section set context level threshold parameters.
threshold available-ip-pool-group

Configures context-level thresholds for IP pool utilization for the system.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold available-ip-pool-group low_thres [ clear high_thres ]
```

`low_thres`
Default: 10
The low threshold IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. `low_thres` can be configured to any integer value between 0 and 100.

`clear high_thres`
Default: 10
The high threshold IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. `high_thres` can be configured to any integer value between 0 and 100. The default is 10.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage
When IP address pools are configured on the system, they can be assigned to a group. IP address pool utilization thresholds generate alerts or alarms based on the utilization percentage of all IP address contained in the pool group during the specified polling interval.
All configured public IP address pools that were not assigned to a group are treated as belonging to the same group. Individual configured static or private pools are each treated as their own group.
Alerts or alarms are triggered for IP address pool utilization based on the following rules:

- **Enter condition:** Actual IP address utilization percentage per pool group ≤ Low Threshold
- **Clear condition:** Actual IP address utilization percentage per pool group > High Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
The following table describes the possible methods for configuring IP pool utilization thresholds:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>

Table 18.
<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context-level</td>
<td>A single IP pool utilization threshold can be configured for all IP pool groups within a given system context. If a single threshold is configured for all pool groups, separate alerts or alarms can be generated for each group. This command configures that threshold.</td>
</tr>
<tr>
<td>IP address pool-level</td>
<td>Each individual IP address pool can be configured with its own threshold. Thresholds configured for individual pools take precedence over the context-level threshold that would otherwise be applied (if configured). In the event that two IP address pools belonging to the same pool group are configured with different thresholds, the system uses the pool configuration that has the greatest low threshold for that group.</td>
</tr>
</tbody>
</table>

**Example**
The following command configures a context-level IP pool utilization low threshold percentage of 10 and a high threshold of 35 for an system using the Alarm thresholding model:

```
threshold available-ip-pool-group 10 clear 35
```
threshold ha-service init-rrq-rcvd-rate

Set an alarm or alert based on the average number of calls setup per second for an HA service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold ha-service init-rrq-rcvd-rate high_thresh[ clear low_thresh]
no threshold ha-service init-rrq-rcvd-rate
```

- **high_thresh**
  - Default: 0
  - The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 1000000.

- **clear low_thresh**
  - Default: 0
  - The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second > High Threshold
- **Clear condition:** Actual number of calls setup per second ≤ Low Threshold

**Example**
The following command configures a number of calls setup per second threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold ha-service init-rrq-rcvd-rate 1000 clear 500
```
**threshold ip-pool-free**

Set an alarm or alert based on the percentage of IP addresses that are unassigned in an IP pool. This command affects all IP pools in the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold ip-pool-free low_thresh [ clear high_thresh ]
```

- **low_thresh**
  Default: 0
  The low threshold percentage of addresses available in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100.

- **clear high_thresh**
  Default: 0
  The high threshold percentage of addresses available in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**
Use this command to set an alert or an alarm when the number of unassigned IP addresses in any pool is equal to or less than a specified percentage of the total number of addresses in the pool. Alerts or alarms are triggered for percentage of IP address pool free based on the following rules:
- **Enter condition:** Actual percentage of IP addresses free per pool £ Low Threshold
- **Clear condition:** Actual percentage of IP addresses free per pool > High Threshold

**Important:** This command is overridden by the settings of the alert-threshold keyword of the `ip pool` command.

**Example**
The following command configures a context-level IP pool percentage of IP addresses that are unused low threshold percentage of 10 and a high threshold of 35 for an system using the Alarm thresholding model:

```
threshold ip-pool-free 10 clear 35
```
threshold ip-pool-hold

Set an alert based on the percentage of IP addresses from an IP pool that are on hold. This command affects all IP pools in the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold ip-pool-hold high_thresh[ clear low_thresh]
```

### high_thresh
Default: 0
The high threshold percentage of addresses on hold in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100.

### clear low_thresh
Default: 0
The low threshold percentage of addresses on hold in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Use this command to set an alert or an alarm when the percentage of IP addresses on hold in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.
Alerts or alarms are triggered for percentage of IP address pool addresses on hold based on the following rules:
- **Enter condition:** Actual percentage of IP addresses on hold per pool > High Threshold
- **Clear condition:** Actual percentage of IP addresses on hold per pool £ Low Threshold

**Important:** This command is overridden by the settings of the `alert-threshold` keyword of the `ip pool` command.

Example
The following command configures a context-level IP pool percentage of IP addresses that are on hold high threshold percentage of 10 and a low threshold of 35 for an system using the Alarm thresholding model:

```
threshold ip-pool-hold 35 clear 10
```
threshold ip-pool-release

Set an alert based on the percentage of IP addresses from an IP pool that are in the release state. This command affects all IP pools in the current context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold ip-pool-release high_thresh[ clear low_thresh]
```

- **high_thresh**
  Default: 0
  The high threshold percentage of addresses in the release state in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100.

- **clear low_thresh**
  Default: 0
  The low threshold percentage of addresses in the release state in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of IP addresses the release state in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool. Alerts or alarms are triggered for percentage of IP addresses in release state per pool based on the following rules:
- **Enter condition:** Actual percentage of IP addresses in the release state per pool > High Threshold
- **Clear condition:** Actual percentage of IP addresses in the release state per pool ≤ Low Threshold

**Important:** This command is overridden by the settings of the alert-threshold keyword of the ip pool command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are in the release state high threshold percentage of 35 and a low threshold of 10 for an system using the Alarm thresholding model:

```
threshold ip-pool-release 35 clear 10
```
threshold ip-pool-release
threshold ip-pool-used

This command sets an alert based on the percentage of IP addresses that have been assigned from an IP pool. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold ip-pool-used high_thresh[ clear low_thresh]

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The high threshold percentage of addresses assigned from an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The low threshold percentage of addresses assigned from an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer value between 0 and 100.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of IP addresses assigned from any pool is equal to or greater than a specified percentage of the total number of addresses in the pool. Alerts or alarms are triggered for percentage of IP address pool addresses used based on the following rules:

- **Enter condition:** Actual percentage of IP addresses used per pool > High Threshold
- **Clear condition:** Actual percentage of IP addresses used per pool £ Low Threshold

**Important:** This command is overridden by the settings of the alert-threshold keyword of the ip pool command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of 35 and a low threshold of 10 for an system using the Alarm thresholding model:

```
threshold ip-pool-used 35 clear 10
```
threshold monitoring

Enables thresholding.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[no] threshold monitoring available-ip-pool-group

no

Disables threshold monitoring for the specified value.

available-ip-pool-group

Enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level. Refer to the `threshold available-ip-pool-group` command, the threshold ip-pool-x commands and the alert-threshold keyword of the `ip pool` command for additional information on these values.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
</table>

Table 19. Thresholding Reporting Mechanisms by Model
Refer to the `threshold poll` command in Global Configuration Mode Commands for information on configuring the polling interval over which IP address pool utilization is monitored.

**Example**

The following command enables threshold monitoring for IP pool thresholds at the context level and the IP address pool level:

```
threshold monitoring available-ip-pool-group
```
threshold pdsn-service init-rrq-rcvd-rate

Set an alarm or alert based on the average number of calls setup per second for a PDSN service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold pdsn-service init-rrq-rcvd-rate [ high_thresh [ clear low_thresh ] ]
```

no threshold pdsn-service init-rrq-rcvd-rate

```
no
```
Deletes the alert or alarm.

```
high_thresh
```
Default: 0
The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 1000000.

```
clear low_thresh
```
Default: 0
The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or less than a specified number of calls per second.
Alerts or alarms are triggered for the number of calls setup per second based on the following rules:
- **Enter condition**: Actual number of calls setup per second > High Threshold
- **Clear condition**: Actual number of calls setup per second £ Low Threshold

Example
The following command configures a number of calls setup per second threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold pdsn-service init-rrq-rcvd-rate 1000 clear 500
```
udr-module active-charging-service

This command creates the User Data Record (UDR) module and enters the UDR Module Active Charging Service Configuration Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

udr-module active-charging-service

Usage
Use this command to create the UDR module for the context, and configure the UDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the EDR module command.

Example

udr-module active-charging-service
The Credit Control Configuration Mode is used to configure prepaid services for Diameter/RADIUS applications.

```
Exec Mode
  active-charging
    service name
      ACS Configuration Mode
      credit-control
        Credit Control Configuration Mode
```
apn-name-to-be-included

This command configures whether the virtual or real APN name is sent in Credit Control Application messaging.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
apn-name-to-be-included { gn | virtual }
default apn-name-to-be-included
```

**Usage**
Use this command to configure the APN information in CCA messages. Virtual APN name can be set to be sent in CCA messages if it is configured in the APN Configuration Mode.

**Example**
The following command sets the virtual APN name to be sent in CCA message:

```
apn-name-to-be-included virtual
```
diameter dictionary

This command configures the Diameter Credit Control dictionary for the Active Charging Service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-
custom12 | dcca-custom13 | dcca-custom14 | dcca-custom15 | dcca-
custom16 | dcca-custom17 | dcca-custom18 | dcca-custom19 | dcca-
custom2 | dcca-custom20 | dcca-
custom3 | dcca-
custom4 | dcca-
custom5 | dcca-
custom6 | dcca-
custom7 | dcca-
custom8 | dcca-
custom9 | standard }
```

**default diameter dictionary**

```plaintext
default
Configures the default setting.
Default: standard dictionary
```

```plaintext
dcca-custom1 ... dcca-custom20
Specifies a custom Diameter dictionary.
```

```plaintext
standard
Specifies the standard Diameter dictionary.
Default: Enabled
```

**Usage**

Use this command to select the Diameter dictionary for Active Charging Service.

**Example**

The following command selects the standard Diameter dictionary:

```plaintext
diameter dictionary standard
```
**diameter gsu-with-only-infinite-quota**

This command configures whether to accept/reject CCA messages that contain `Granted-Service-Unit` AVP with only infinite quota grants from the server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
diameter gsu-with-only-infinite-quota { accept-credit-control-answer | reject-credit-control-answer }
```

**Usage**

Use this command to accept/reject CCA messages that contain `Granted-Service-Unit` AVP with only infinite quota grants from the server.

**Example**

The following command specifies to accept CCA with `Granted-Service-Unit` AVP containing only Infinite quota:

```
diameter gsu-with-only-infinite-quota accept-credit-control-answer
```

The following command configures to reject `Granted-Service-Unit` that contains only Infinite quota:

```
diameter gsu-with-only-infinite-quota reject-credit-control-answer
```
diameter ignore-returned-rulebase-id

This command configures to accept/ignore rulebase ID in *Rulebase-Id* AVP returned by the Diameter server in CCA message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] diameter ignore-returned-rulebase-id
```

- **default**
  Configures the default setting.
  Default: accept

- **no**
  Specifies to accept the rulebase ID received from Diameter server in CCA.

**Usage**
Use this command to ignore/accept rulebase ID returned from the Diameter server in CCA.

**Example**
This following command specifies to ignore rulebase ID returned from Diameter server in CCA:

```
diameter ignore-returned-rulebase-id
```
diameter mscc-per-ccr-update

This command configures sending single/multiple Multiple-Services-Credit-Control (MSCC) AVP in CCR-U messages.

Important: This command is only available in StarOS 8.3 and later.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter mscc-per-ccr-update { multiple | single }
default diameter mscc-per-ccr-update

default
Configures the default setting.
Default: multiple

multiple
Specifies sending multiple Multiple-Services-Credit-Control AVP in a single CCR-U message.

single
Specifies sending only one Multiple-Services-Credit-Control AVP in a CCR-U message.

Usage
Use this command to configure sending single/multiple Multiple-Services-Credit-Control AVP in CCR-U messages.

Example
The following command configures sending a single MSCC AVP in CCR-U messages:
diameter mscc-per-ccr-update single
diameter origin host

This command is obsolete. See the diameter origin endpoint command.
diameter origin endpoint

This command configures the Diameter Credit Control Origin Endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
diameter origin endpoint endpoint_name [ realm realm_name ]
no diameter origin endpoint
```

---

**no**
Removes the Diameter Credit Control Origin Endpoint configuration.

**endpoint_name**
Specifies the Diameter Credit Control Origin Endpoint.
`endpoint_name` must be the endpoint’s name, and an alpha and/or numeric string of 1 through 63 characters in length.

**realm realm_name**
Specifies the Diameter Credit Control Realm ID.
`realm_name` must be a string of 1 through 127 characters in length.

**Usage**
Use this command to configure the Diameter Credit Control Origin Endpoint.
The endpoint to configure should be pre-configured. For information on creating and configuring a Diameter endpoint, in the Context Configuration Mode, see the `diameter endpoint` command.

**Example**
The following command configures a Diameter Credit Control Origin Endpoint named `test`:
```
diameter origin endpoint test
```
diameter peer-select

This command configures the Diameter credit control primary and secondary hosts for DCCA.

Product
All

Privilege
Security Administrator, Administrator

Syntax
In StarOS 8.x:

diameter peer-select peer peer_name [ realm realm_name ] [ secondary-peer sec_peer_name [ realm realm_name ] ] [ imsi-based start-value imsi_start_value end-value imsi_end_value ]

no diameter peer-select [ imsi-based start-value imsi_start_value end-value imsi_end_value ]

In StarOS 9.0 and later for UMTS deployments:

diameter peer-select peer peer_name [ realm realm_name ] [ secondary-peer sec_peer_name [ realm realm_name ] ] [ imsi-based { [ prefix | suffix ] imsi/prefix/suffix_start_value } [ to imsi/prefix/suffix_end_value ] ]

no diameter peer-select [ imsi-based { [ prefix | suffix ] imsi/prefix/suffix_start_value } [ to imsi/prefix/suffix_end_value ] ]

no
Removes previously configured Diameter credit control peer selection setting.

peer peer_name
Specifies the primary host name.
peer_name must be an alpha and/or numeric string of 1 through 63 characters in length, and can contain punctuation characters.

imsi-based start-value imsi_start_value end-value imsi_end_value
Available only in StarOS 8.3 and earlier releases.
Specifies peer selection based on International Mobile Subscriber Identification (IMSI) range.
start-value imsi_start_value specifies the start of range in integer value of IMSI, and end-value imsi_end_value specifies the end of range in integer value of IMSI.

to imsi/prefix/suffix_end_value
In this release, available only for UMTS deployments.
Specifies peer selection based on IMSI prefix or suffix or IMSI range.
prefix: Specifies the prefix range
suffix: Specifies the suffix range
**diameter peer-select**

**imsi/prefix/suffix_start_value**: Specifies the IMSI/prefix/suffix start value. `prefix/suffix` must be IMSI prefix/suffix, and must be an integer from 1 through 15 characters in length.

**imsi/prefix/suffix_end_value**: Specifies the IMSI/prefix/suffix end value. `prefix/suffix` must be IMSI prefix/suffix, and must be an integer from 1 through 15 characters in length, and must be greater than the start value.

**Important**: If prefix/suffix is used, the lengths of both start and end prefix/suffix must be equal. If the `prefix` or `suffix` keyword is not specified, it will be considered as suffix.

```
realm realm_name
```

The `realm_name` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters. The realm may typically be a company or service name.

```
secondary-peer sec_peer_name
```

Specifies a name for the secondary host to be used for failover processing. When the route-table does not find an AVAILABLE route, the secondary host performs a failover processing if the `diameter session failover` command is set.

`sec_peer_name` must be an alpha and/or numeric string of 1 through 63 characters in length, and can contain punctuation characters.

**Usage**

Use this command to configure Diameter credit control host selection.

If the `diameter peer-select` command is not configured, and if multiple peers are configured in the endpoint, the available peers configured in the endpoint are automatically chosen in a load-balanced round-robin manner.

In StarOS 9.0 and later, a prefix or suffix of IMSI or IMSI range can be configured. If prefix or suffix keyword is not specified, it will be considered as suffix. Up to 64 peer selects can be configured. At any time either prefix or suffix mode can be used in one DCCA config. If the prefix/suffix mode is used, the start and end prefix/suffix lengths must be equal.

StarOS 9.0 and later supports peer selection using prefix or suffix of IMSI or IMSI range. Subscribers are now assigned to a primary OCS instance based on the value of the IMSI prefix or suffix of a length of 1 to 15 digits. If the prefix or suffix keyword is not specified, it will be considered as suffix. Up to 64 peer selects can be configured. At a time either prefix or suffix mode can be used in one DCCA config. If prefix or suffix mode is used, the lengths of all prefix/suffix must be equal.

Each primary OCS may have a designated secondary OCS in case of failure of the primary. It will be the responsibility of the GGSN to use the appropriate secondary OCS in case of primary failure. The secondary OCS for each primary OCS will be one of the existing set of OCSs.

**Example**

The following command configures a Diameter credit control peer named `test` and the realm `companyx`:

```
diameter peer-select peer test realm companyx
```

The following command configures IMSI-based Diameter credit control peer selection in the IMSI range of 1234567890 to 1234567899:

```
diameter peer-select peer star imsi-based start-value 1234567890 end-value 1234567899
```

The following command configures IMSI-based DCCA peer selection with IMSI suffix of 100 through 200:
diameter peer-select peer test_peer realm test.realm secondary-peer
test_sec.realm realm test.realm2 imsi-based suffix 100 to 200
diameter pending-timeout

This command configures the maximum time period to wait for response from a Diameter peer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter pending-timeout duration

default diameter pending-timeout

default
Disables DCCA resending message at pending-timeout.

duration
Specifies the timeout duration in seconds. duration must be an integer from 1 through 300.

after-expiry-try-secondary-host
This keyword is deprecated. This can now be managed using the retry-after-tx-expiry and go-offline-after-tx-expiry keywords in the failure-handling command.

Usage

Use this command to set the maximum time for Diameter credit control to receive a response from its peer. DCCA refers to this as the Tx Timer. Typically, this should be configured to a value smaller than the response-timeout value of Diameter Endpoint Configuration Mode. That value is typically too large for DCCA's purposes.

If DCCA gets a "no available routes" error before pending-timeout expires, then DCCA tries to send to the secondary host (if one has been configured). If DCCA gets no response and pending-timeout expires, then DCCA either tries the secondary host or gives up. This can now be managed using the failure-handling command.

If routing has failed, i.e., the attempt to the primary host, as well as, the attempt to the secondary host (if that has been configured), then the processing configured by the failure-handling CLI command is performed.

The routing (i.e., returning a good response, no response or an error response such as "no available routes") is controlled by Diameter Endpoint Configuration Mode. That uses a watchdog timer (called Tw Timer) to attempt a different route to a host. Multiple routes could be attempted. If there's no response before the endpoint's configured response-timeout expires, then "no available routes" is the routing result. The routing logic remembers the status of routes, so it can return "no available routes" immediately, without using any timers.

The default case will disable DCCA resending message at Tx (pending-timeout). So messages are retried only at Tw (device watchdog timeout) by diabase or at response-timeout by DCCA.
Example
The following command configures a Diameter Credit Control Pending Timeout of 20:

```
diameter pending-timeout 20
```
diameter result-code

This command enables sending GTP Create-PDP-Context-Rsp message with cause code based on the DCCA result code.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter result-code { authorization-rejected | user-unknown } use-gtp-cause-code { authentication-failure | no-resource-available }

default diameter result-code { authorization-rejected | user-unknown } use-gtp-cause-code

<table>
<thead>
<tr>
<th>authorization-rejected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result code received as DIAMETER_AUTHORIZATION_REJECTED(5003).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>user-unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result code received as DIAMETER_USER_UNKNOWN(5030).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>use-gtp-cause-code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause code to be sent in GTP response.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>authentication-failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>To send GTP cause code GTP_USER_AUTHENTICATION_FAILED in GTP response.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no-resource-available</th>
</tr>
</thead>
<tbody>
<tr>
<td>To send GTP cause code GTP_NO_RESOURCES_AVAILABLE in GTP response (default cause code).</td>
</tr>
</tbody>
</table>

Usage
On receiving result-code as AUTHORIZATION-REJECTED or DIAMETER_USER_UNKNOWN from DCCA server, the cause code can either be sent as GTP_NO_RESOURCE_AVAILABLE or GTP_AUTHENTICATION_FAILED in GTP create-PDP-Context response message, based on this CLI configuration. By default, GTP_NORESOURCEAVAILABLE is sent.

Example
The following command sets the deny cause as user authentication failure when the CCA-Initial has the result code DIAMETER_AUTHORIZATION_REJECTED(5003):

diameter result-code authorization-rejected use-gtp-cause-code authentication-failure
diameter send-ccri

This command configures when to send CCR-Initial for the subscriber session.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter send-ccri { session-start | traffic-start }
default diameter send-ccri

default
Configures the default setting.
Default: session-start

session-start
Specifies to send CCR-I when the PDP context is being established (on receiving Create-PDP-Context-Request).

traffic-start
Specifies to delay sending CCR-I until the first data packet received from the subscriber.

Usage
Use this command to configure when to send CCR-Initial for the subscriber session.

Example
The following command configures to send CCR-I on traffic detection and not on context creation:
diameter send-ccri traffic-start
diameter session failover

This command enables/disables Diameter Credit Control Session Failover. When enabled, the secondary peer is used in the event the main peer is unreachable.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] diameter session failover
```

- **default**
  Configures the default setting.
  Default: Depends on the `failure-handling` configuration

- **no**
  If the primary server is not reachable, failover is not triggered and the session is torn down. No failover action is taken.

**Usage**

Use this command to enable/disable Diameter Credit Control Session Failover.

The `failure-handling` configuration comes into effect only if `diameter session failover` is present in the configuration. The failover can be overridden by the server in the response message, and it takes precedence.

**Example**

The following command enables Diameter Credit Control Session Failover:

```
diameter session failover
```
end

Returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
**exit**

Exits the current mode and returns to the Active Charging Service Configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the Active Charging Service Configuration mode.
failure-handling

This command configures the Diameter Credit Control Failure Handling (CCFH) behavior in the event of communication failure with the prepaid server.

Product
All

Privilege
Security Administrator, Administrator

Syntax


default failure-handling [ initial-request | terminate-request | update-request ]

default failure-handling [ initial-request | terminate-request | update-request ]

Configures the default CCFH setting:
initial-request: The default setting is terminate.
update-request: The default setting is retry-and-terminate.
terminate-request: The default setting is retry-and-terminate.

initial-request
Specifies the message type as CCR-Initial.

terminate-request
Specifies the message type as CCR-Terminate.

update-request
Specifies the message type as CCR-Update.

continue
Specifies the CCFH setting as continue. The online session is converted into offline session. The associated PDP Context is established (new sessions) or not released (ongoing sessions).

retry-and-terminate
Specifies the CCFH setting as retry-and-terminate. The user session will continue for the duration of one retry attempt with the prepaid server. In case there is no response from both primary and secondary servers the session is torn down.

terminate
Specifies the CCFH setting as terminate. All type of sessions (initial or update) are terminated in case of failure.
go-offline-after-tx-expiry
Specifications to start offline charging after Tx expiry.

retry-after-tx-expiry
Specifications to retry after Tx expiry. Enables secondary-host, if up, to take over after Tx expiry.

Usage
Use this command to select the CCFH behavior. The specified behavior is used for sessions when no behavior is specified by the prepaid server. By default, the CCFH is taken care at response-timeout except for terminate setting.

If the Credit-Control-Failure-Handling AVP is received from the server, the received setting will be applied to all the message types.

The following table indicates the CCFH behavior for the combination of different CCFH settings, and the corresponding CLI commands.

<table>
<thead>
<tr>
<th>CCFH Setting</th>
<th>CLI Command</th>
<th>Behavior at Tx</th>
<th>Behavior at RT</th>
<th>Secondary is Up</th>
<th>Secondary is Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial-request Message Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue</td>
<td>initial-request continue</td>
<td>N/A</td>
<td>Continue</td>
<td>Secondary takes over after RT</td>
<td>Offline after another RT. No more quota requests are performed for any rating group within the session after DCCA failure (even if connectivity to DCCA is restored)</td>
</tr>
<tr>
<td></td>
<td>initial-request continue go-offline-after-tx-expiry</td>
<td>Offline</td>
<td>N/A</td>
<td>Offline at Tx</td>
<td>Offline at Tx</td>
</tr>
<tr>
<td></td>
<td>initial-request continue retry-after-tx-expiry</td>
<td>Continue</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Offline after another Tx</td>
</tr>
<tr>
<td>Retry-and-terminate</td>
<td>initial-request retry-and-terminate</td>
<td>N/A</td>
<td>Retry</td>
<td>Secondary takes over after RT</td>
<td>Terminate after another RT</td>
</tr>
<tr>
<td></td>
<td>initial-request retry-and-terminate retry-after-tx-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Terminate after another Tx</td>
</tr>
<tr>
<td>Terminate</td>
<td>initial-request terminate</td>
<td>Terminate</td>
<td>N/A</td>
<td>Terminate after Tx</td>
<td>Terminate after Tx</td>
</tr>
<tr>
<td>Update-request Message Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue</td>
<td>update-request continue</td>
<td>N/A</td>
<td>Continue</td>
<td>Secondary takes over after RT</td>
<td>Offline after another RT</td>
</tr>
<tr>
<td>CCFH Setting</td>
<td>CLI Command</td>
<td>Behavior at Tx</td>
<td>Behavior at RT</td>
<td>Secondary is Up</td>
<td>Secondary is Down</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>update-request continue go-offline-after-tx-expiry</td>
<td>Offline</td>
<td>N/A</td>
<td>Offline at Tx</td>
<td>Offline at Tx</td>
</tr>
<tr>
<td></td>
<td>update-request continue retry-after-tx-expiry</td>
<td>Continue</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Offline after another Tx</td>
</tr>
<tr>
<td>Retry-and-terminate</td>
<td>update-request retry-and-terminate</td>
<td>N/A</td>
<td>Retry</td>
<td>Secondary takes over after RT</td>
<td>Sends CCR-T after another RT</td>
</tr>
<tr>
<td></td>
<td>update-request retry-and-terminate retry-after-tx-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Sends CCR-T after another Tx</td>
</tr>
<tr>
<td>Terminate</td>
<td>update-request terminate</td>
<td>Terminate</td>
<td>N/A</td>
<td>Sends CCR-T after Tx</td>
<td>Sends CCR-T after Tx</td>
</tr>
</tbody>
</table>

**Terminate-request Message Type**

| Continue | terminate-request continue | N/A | Retry | CCR-T is sent to secondary after RT | Terminate after another RT |
|          | terminate-request continue go-offline-after-tx-expiry | Retry | N/A | CCR-T is sent to secondary after Tx | Terminate after another Tx |
|          | terminate-request continue retry-after-tx-expiry | Retry | N/A | CCR-T is sent to secondary after Tx | Terminate after another Tx |
| Retry-and-terminate | terminate-request retry-and-terminate | N/A | Retry | CCR-T is sent to secondary after RT | Terminate after another RT |
|          | terminate-request retry-and-terminate retry-after-tx-expiry | Retry | N/A | CCR-T is sent to secondary after Tx | Terminate after another Tx |
| Terminate | terminate-request terminate | Terminate | N/A | Terminate after Tx | Terminate after Tx |

**Example**
The following command sets the Credit Control Failure Handling behavior for initial request message type to retry-and-terminate:

`failure-handling initial-request retry-and-terminate`
mode

This command configures the Prepaid Credit Control mode to RADIUS or Diameter.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
mode { diameter | radius }
```

default mode

default
Configures the default prepaid credit control mode.
Default: Diameter

diameter
Enables Diameter Credit Control Application (DCCA) for prepaid charging.

radius
Enables RADIUS Credit Control for prepaid charging.

Usage
Use this command to configure the prepaid charging application mode between Diameter or RADIUS credit control.

Example
The following command specifies to use RADIUS prepaid credit control application:

```
mode radius
```
pending-traffic-treatment

This command controls the pass/drop treatment of traffic while waiting for definitive credit information from the server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
pending-traffic-treatment { { forced-reauth | trigger | validity-expired } drop | pass } | { { noquota | quota-exhausted } buffer | drop | pass } }

default pending-traffic-treatment { forced-reauth | noquota | quota-exhausted | trigger | validity-expired }
```

---

**default**
Configures the default setting.
Default: drop

---

**forced-reauth**
Sets the Diameter credit control pending traffic treatment to forced reauthorization.

---

**trigger**
Sets the Diameter credit control pending traffic treatment to trigger.

---

**validity-expired**
Sets the Diameter credit control pending traffic treatment to validity expired.

---

**noquota**
Sets the Diameter credit control pending traffic treatment to no quota.

---

**quota-exhausted**
Sets the Diameter credit control pending traffic treatment to quota exhausted.

---

**buffer**
Specifies to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic passed.

---

**drop**
Specifies to drop any traffic when there is no quota present.

---

**pass**
Specifies to pass all traffic more or less regardless of quota state.
Usage
Use this command to set the Diameter credit control pending traffic treatment while waiting for definitive credit information from the server.
This CLI command is different than the `failure-handling` CLI command, which specifies behavior in the face of an actual timeout or error, as opposed to the behavior while waiting. See also the `buffering-limit` CLI command in Active Charging Service Configuration Mode.

Example
The following command sets the Diameter credit control pending traffic treatment to drop any traffic when there is no quota present:

```
pending-traffic-treatment noquota drop
```
### quota

This command is used to set various time-based quotas in the prepaid credit control service.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax**

```plaintext
{ default | no } quota { holding-time | validity-time }
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>holding-time</td>
<td>Specifies the Quota Holding Time (QHT). holding_time must be an integer from 1 through 4000000000.</td>
</tr>
<tr>
<td>validity-time</td>
<td>Specifies the validity lifetime of the quota. validity_time must be an integer from 1 through 65535.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the prepaid credit control quotas.

**Example**

The following command sets the prepaid credit control request holding time to 30000 seconds:

```plaintext
quota holding-time 30000
```
quota request-trigger

This command is used to set the action on packets used from request trigger on crossing threshold limit of subscriber quota in the prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
quota request-trigger { exclude-packet-causing-trigger | include-packet-causing-trigger }
{ default | no } quota request-trigger
```

- **default**
  Configures the default setting.
  Default: Disabled

- **no**
  Disables time threshold for prepaid credit control quota.

- **exclude-packet-causing-trigger**
  Default: Disabled
  This option excludes the packets causing threshold limit violation trigger in accounting.

- **include-packet-causing-trigger**
  Default: Disabled
  This option includes the packets causing threshold limit violation trigger in accounting.

Usage
Use this command to set the action of packets causing threshold limit violation for prepaid credit control quotas.

Example
The following command sets the system to exclude the packets causing threshold limit triggers from accounting of prepaid credit of a subscriber:

```
quota request-trigger exclude-packet-causing-trigger
```
quota time-threshold

This command configures the time threshold limit for subscriber quota in the prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

quota time-threshold { abs_time_value | percent percent_value }
{ default | no } quota time-threshold

default
Configures the default setting.
Default: Disabled

no
Disables time threshold for prepaid credit control quota.

abs_time_value
Default: 0 (Disabled)
Specifies the absolute threshold time in seconds for configured time quota in prepaid credit control charging.
abs_time_value must be an integer from 1 through 86400. To disable this assign 0.

percent percent_value
Specifies the time threshold value in percentage of configured time quota in DCCA.
percent_value must be an integer from 1 through 100.

Usage
Use this command to set the time threshold for prepaid credit control quotas.

Example
The following command sets the prepaid credit control time threshold to 400 seconds:
quota time-threshold 400
quota units-threshold

This command is used to set the unit threshold limit for subscriber quota in the prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
quota unit-threshold { abs_unit_value | percent percent_value }
{ default | no } quota units-threshold
```

default
Configures the default setting.
Default: Disabled

no
Disables unit threshold for DCCA quota.

abs_unit_value
Default: 0 (Disabled)
Specifies the absolute threshold value in units for the configured units quota in prepaid credit control application.
abs_unit_value must be an integer from 1 through 4000000000. To disable this assign 0.

percent percent_value
Specifies the time threshold value in percentage of configured units quota in DCCA.
percent_value must be an integer from 1 through 100.

Usage
Use this command to set the units threshold for prepaid credit control quotas.

Example
The following command sets the prepaid credit control time threshold to 160400 units:

```
quota units-threshold 160400
```
quota volume-threshold

This command is used to set the volume threshold limit for subscriber quota in the prepaid credit control service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
quota volume-threshold { abs_vol_value | percent percent_value }

{ default | no } quota volume-threshold
```

**default**
Configures the default setting.
Default: Disabled

**no**
Disables volume threshold for prepaid credit control quota.

**abs_vol_value**
Default: 0 (Disabled)
Specifies the absolute threshold volume in bytes to configured volume quota in prepaid credit control.
`abs_vol_value` must be an integer from 1 through 4000000000. To disable this assign 0.

**percent percent_value**
Specifies the volume threshold value in percentage of configured volume quota in prepaid credit control.
`percent_value` must be an integer from 1 through 100.

**Usage**
Use this command to set the volume threshold for prepaid credit control quotas.

**Example**
The following command sets the prepaid credit control volume threshold to 160400 bytes:

```
quota volume-threshold 160400
```
radius usage-reporting-algorithm

This command configures the usage reporting algorithm for RADIUS prepaid using DCCA.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
radius usage-reporting-algorithm { cumulative | relative }
default radius usage-reporting-algorithm
```

- **default**
  Configures the default setting.
  Default: Cumulative

- **cumulative**
  Specifies that the total accumulated usage of quota be reported in every accounting interim.

- **relative**
  Specifies that the quota usage be reported per accounting interim. I.e., since the previous usage report.

Usage

Use this command to configure the usage reporting algorithm for RADIUS prepaid using DCCA.

Example

The following command configures the usage reporting algorithm for RADIUS prepaid using DCCA to `relative`:
```
radius usage-reporting-algorithm relative
```
**timestamp-rounding**

This command configures how to convert exact time into the units that are used in quotas.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
timestamp-rounding { ceiling | floor | roundoff }
default timestamp-rounding
```

- **default**
  
  Sets the default timestamp-rounding setting.
  
  Default: `roundoff`

- **ceiling**
  
  This keyword round-off to the smallest integer greater than the fraction.
  
  If the fractional part of the seconds is greater than 0, then this keyword adds 1 to the number of seconds and discard the fraction.

- **floor**
  
  This keyword always discards the fractional part of the second.

- **roundoff**
  
  This keyword sets the fractional part of the seconds to nearest integer value. If fractional value is greater than or equal to 0.5 it adds 1 to the number of seconds and discards the fractional part of second.

**Usage**

Use this command to configure how to convert exact time into the units that are used in quotas for CCA charging.

The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (i.e., $2 - 1 = 1$).

**Example**

The following command sets the CCA timestamp to nearest integer value second; i.e. 34:12.23 to 34:12.00:

```
timestamp-rounding roundoff
```
trigger type

This command enables or disables triggering a credit reauthorization when the named values in the subscriber session changes.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] trigger type { cellid | lac | qos | rat | sgsn } +

default trigger type

default
Sets the default trigger type setting.

no
Removes the previously configured trigger type.

cellid
Sets the trigger based on change in cell identity or service area code (SAC)

lac
Sets the trigger based on change in Location Area Code.

qos
Sets the trigger based on change in the Quality of Service (QoS).

rat
Sets the trigger based on change in the Radio Access Technology (RAT).

sgsn
Sets the trigger based on change in the IP address of SGSN.

+
Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Use this command to set the credit control reauthorization trigger.

Example
The following command selects a credit control trigger as **lac**:

```
trigger type lac
```
usage-reporting

This command configures the ACS Credit Control usage reporting type.

Product
All

Privilege
Security Administrator, Administrator

Syntax

Usage
Use this command to configure reporting usage only for granted quota. On issuing this command, the Used-Service-Unit AVP will report quotas based on grant i.e., only the quotas present in the Granted-Service-Unit AVP.
With this command only the units for which the quota was granted by the DCCA server will be reported irrespective of the reporting reason.

Example
The following command configures to report usage based only on granted quota:

```bash
usage-reporting quotas-to-report based-on-grant
```
Chapter 39
Credit Control Service Configuration Mode Commands

The Credit Control Service Configuration Mode is used to create and manage Credit Control Service.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          credit-control-service name
            Credit Control Service Configuration Mode
```
**diameter dictionary**

This command configures the Diameter dictionary to be used for this Credit Control Service instance.

**Product**
- All

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
diameter dictionary { custom1 | standard }

default diameter dictionary

default
Configures the default setting.


dictionary { custom1 | standard }
Specifies the Diameter dictionary to be used.
custom1: Specifies the custom dictionary custom1.
standard: Specifies the standard dictionary.
```

**Usage**

Use this command to configure the Diameter dictionary to be used for this Credit Control Service instance.

**Example**

The following command configures the standard Diameter dictionary:

```
diameter dictionary standard
```
diameter endpoint

This command configures the Diameter Credit Control Interface Endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
diameter endpoint endpoint_name
{ default | no } diameter endpoint
```

- **default**
  - Configures the default setting.

- **no**
  - Removes the previous Diameter endpoint configuration.

- **endpoint_name**
  - Specifies the Diameter endpoint name.
  - `endpoint_name` must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

Use this command to configure the Diameter Credit Control Interface Endpoint.

**Example**

The following command configures the Diameter Credit Control Interface Endpoint named `test135`:

```
diameter endpoint test135
```
**end**

This command exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to change to the Exec mode.
exit

This command exits the current configuration mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
failure-handling

This command configures the Diameter failure handling behavior.

Product
All

Privilege
Security Administrator, Administrator

Syntax

failure-handling { initial-request | terminate-request | update-request } {
diameter-result-code result_code [ to result_code ] | peer-unavailable |
request-timeout } action { continue | retry-and-continue | retry-and-terminate |
terminate }

{ default | no } failure-handling { initial-request | terminate-request |
update-request } { diameter-result-code result_code [ to result_code ] | peer-
unavailable | request-timeout }

default
Configures the default setting.

no
Removes the previous failure handling configuration.

initial-request | terminate-request | update-request
initial-request: Specifies failure handling for Initial Request.
terminate-request: Specifies failure handling for Terminate Request.
update-request: Specifies failure handling for Update Request.

diameter-result-code | peer-unavailable | request-timeout
diameter-result-code result_code [ to result_code ]: Specifies Diameter result code(s)
for failure handling.
result_code must be an integer from 3000 through 9999.
to result_code: Specifies the range of Diameter result codes.
peer-unavailable: Specifies failure handling for peer being unavailable.
request-timeout: Specifies failure handling for request timeouts.

action { continue | retry-and-continue | retry-and-terminate | terminate }

Specifies the failure handling action.
continue: Continue the session without credit control.
retry-and-continue: Retry and, even if credit control is not available, continue.
retry-and-terminate: Retry and then terminate.
terminate: Terminate the session.
Usage

Use this command to configure the Diameter failure handling behavior.

Example

The following command configures initial request failure handling behavior for Diameter result codes 3001 to 4001 with terminate action:

```plaintext
failure-handling initial-request diameter-result-code 3001 to 4001 action terminate
```
request timeout

This command configures the timeout period for Diameter requests.

Product
All

Privilege
Security Administrator, Administrator

Syntax

request timeout timeout

{ default | no } request timeout

- default
  Configures the default setting.

- no
  Removes the previous request timeout configuration.

- timeout
  Specifies the timeout period in seconds, and must be an integer from 1 through 300.

Usage
Use this command to configure the Diameter request timeout value, after which the request is deemed to have failed. This timeout is an overall timeout, and encompasses all retries with the server(s).

Example
The following command configures the timeout period to 150 seconds:

request timeout 150
Chapter 40
Crypto Group Configuration Mode Commands

The Crypto Group Configuration Mode is used to configure crypto (tunnel) groups for providing fail-over redundancy for IPSec tunnels to packet data networks (PDNs).

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the context configuration mode.
**match address**

Associates an access control list (ACL) to the crypto group.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match address acl_name [ preference ]
no match address acl_name
```

<table>
<thead>
<tr>
<th>no</th>
<th>Deletes a previously configured ACL association.</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl_name</td>
<td>The name of the ACL being matched to the crypto group.</td>
</tr>
<tr>
<td>preference</td>
<td>The priority of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL. preference can be configured to any integer value from 0 to 4294967295. &quot;0&quot; is the highest priority. If multiple ACLs are assigned the same priority, the last one entered will be used first.</td>
</tr>
</tbody>
</table>

**Important**: The priorities are only compared for ACLs matched to other groups or to policy ACLs (those applied to the entire context).

**Usage**

IP ACLs are associated with crypto groups using this command. Both the crypto group and the ACLs must be configured in the same context. ISAKMP crypto maps can then be associated with the crypto group. This allows user traffic matching the rules of the ACL to be handled according to the policies configured as part of the crypto map.

**Example**
The following command associates an ACL called *corporate_acl* to the crypto group:

```
match address corporate_acl
```
match ip pool

Matches the specified IP pool to the current crypto group. This command can be used multiple times to match more than one IP pool.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```markdown
match ip pool pool-name pool_name
no match ip pool pool-name pool_name
```

**Usage**
Use this command to set the names of IP pools that should be matched in the current crypto group.

**Example**
The following command sets a rule for the current crypto group that will match an IP pool named **ippool1**:

```markdown
match ip pool pool-name ippool1
```
switchover

switchover auto [ do-not-revert ]

no switchover auto

no
Disables the automatic switchover of tunnels. This applies to both primary-to-secondary and secondary-to-
primary switches.

auto
Default: Enabled
Allows the automatic switchover of tunnels.

do-not-revert
Default: Disabled
Disables the automatic switchover of secondary tunnels to primary tunnels.

Usage
This command configures the fail-over options for the Redundant IPSec Fail-over feature.
If the automatic fail-over options are disabled, tunneled traffic must be manually switched to the alternate
tunnel (or manually activated if no alternate tunnel is configured and available) using the following command
in the Exec Mode:
crypto-group group_name activate { primary | secondary }
For a definition of this command, see the crypto-group section of the Exec Mode Commands chapter of this
guide.

Example
The following command disables the automatic secondary-to-primary switchover:

switchover auto do-not-revert
Chapter 41
Crypto Map Dynamic Configuration Mode Commands

The Crypto Map Dynamic Configuration Mode is used to configure IPSec tunnels that are created as needed to facilitate subscriber sessions using Mobile IP or L2TP.

Modification(s) to an existing dynamic crypto map configuration will not take effect until the related security association has been cleared. Refer to the clear crypto security-association command located in the Exec Mode Commands chapter of the Command Line Interface Reference for more information.
end

Returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the DYnamic Crypto Map configuration mode and returns to the context configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
exit
```

Usage

Return to the context configuration mode.
set

Configures parameters for the dynamic crypto map.

Product
PDSN, HA, GGSN, PDIF

Privilege
Security Administrator, Administrator

Syntax

```bash
set { control-dont-fragment { clear-bit | copy-bit | set-bit } | isakmp natt [keepalive time] | pfs { group1 | group2 | group5 } | phase1-idtype { id-key-id | ipv4-address } [ mode { aggressive | main } ] | phase2-idtype { ipv4-address | ipv4-address-subnet } | security-association lifetime { keepalive | kbyte kbytes | seconds secs } | transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ] }
no set { pfs | security-association lifetime { keepalive | kilo-bytes kbytes | seconds secs } | phase1-idtype | phase2-idtype | transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ] }
```

no

Deletes the specified parameter or resets the specified parameter to the default value.

---

control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet. Options are:

- **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
- **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).

isakmp natt [keepalive time]

Enable IPsec NAT Traversal.

**keepalive time**: The time to keep the NAT connection alive in seconds. **time** must be an integer of from 1 through 3600 seconds. It must be an integer of from 1 through 3600 seconds.

pfs { group1 | group2 | group5 }

Specifies the modp Oakley group (also known as the Diffie-Hellman (D-H) group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).

- **group1**: Diffie-Hellman Group1 (768-bit modp)
- **group2**: Diffie-Hellman Group2 (1024-bit modp)
- **group5**: Diffie-Hellman Group5 (1536-bit modp)

phase1-idtype { id-key-id | ipv4-address } [ mode { aggressive | main } ]

Sets the IKE negotiations Phase 1 payload identifier.
Default: ipv4-address

**id-key-id**: Use ID_KEY_ID as the Phase 1 payload identifier.

**ipv4-address**: Use IPv4_ADDR as the Phase 1 payload identifier.

**mode** { aggressive | main }: Specify the IKE mode.

---

**phase2-idtype** { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier.

Default: ipv4-address-subnet

**ipv4-address**: Use IPv4_ADDR as the Phase 2 payload identifier.

**ipv4-address-subnet**: Use IPv4_ADDR_SUBNET as the Phase 2 payload identifier.

---

**security-association lifetime** { keepalive | kilo-bytes kbytes | seconds secs }

Defaults:

- **keepalive**: Disabled
- **kilo-bytes**: 4608000 kbytes
- **seconds**: 28800 seconds

This keyword specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.

- **keepalive**: The SA lifetime expires only when a keepalive message is not responded to by the far end.

- **kilo-bytes** kbytes : This specifies the amount of data in kilobytes to allow through the tunnel before the SA lifetime expires. kbytes must be an integer from 2560 through 4294967294.

- **seconds** secs : The number of seconds to wait before the SA lifetime expires. secs must be an integer from 1200 through 86400.

---

**Important**: If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map’s SA lifetime (either in terms of kilobytes or seconds), then the **keepalive** parameter must be configured.

---

**transform-set** transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]

This keyword specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command **crypto ipsec transform-set** for information on creating transform sets.

You can repeat this keyword up to 6 times on the command line to specify multiple transform sets. **transform_name** is the name of the transform set and must be an alpha and/or numeric string from 1 to 127 characters and is case sensitive.

---

**Usage**

Use this command to set parameters for a dynamic crypto map.

---

**Example**

The following command sets the PFS group to Group1:
set pfs group1

The following command sets the SA lifetime to 50000 KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to 10000 seconds:

```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```

The following command defines transform sets tset1 and tset2.

```
set transform-set tset1 transform-set tset2
```
Chapter 42
Crypto Map IKEv1 Configuration Mode Commands

The Crypto Map IKEv1 Configuration Mode is used to configure properties for IPSec tunnels that will be created using the Internet Key Exchange (IKE) that operates within the framework of the Internet Key Exchange version 1 (IKEv1).

Modification(s) to an existing IKEv1 crypto map configuration will not take effect until the related security association has been cleared. Refer to the clear crypto security-association command located in the Exec Mode Commands chapter of the Command Line Interface Reference for more information.

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

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
**match address**

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

**Product**

PDSN, HA, GGSN, SCM

**Privilege**

Security Administrator, Administrator

**Syntax**

```
match address acl_name priority
no match address
```

**no**

Removes a previously matched ACL.

**acl_name**

The name of the ACL that the crypto map is to be matched with. `acl_name` can be from 1 to 79 alpha and/or numeric characters and is case sensitive.

**priority**

Default: 0

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL.

The preference can be configured to any integer value from 0 to 4294967295. “0” is the highest priority.

**Important:** The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

**Usage**

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

**Example**

The following command sets the crypto map ACL to the ACL named `ACLlist1` and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```
match crypto group

Matches or associates the crypto map a crypto group configured in the same context.

**Product**
PDSN, HA, GGSN, SCM

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match crypto group group_name { primary | secondary }
no match crypto group group_name
```

**no**
Deletes a previously configured crypto group association.

**group_name**
The name of the crypto group and can consist of from 1 to 127 alpha and/or numeric characters in length and is case sensitive.

**primary**
Specifies that the policies configured as part of this crypto map will be used for the primary tunnel in the Redundant IPSec Tunnel Failover feature.

**secondary**
Specifies that the policies configured as part of this crypto map will be used for the secondary tunnel in the Redundant IPSec Tunnel Failover feature.

**Usage**
Use this command to dictate the primary and secondary tunnel policies used for the Redundant IPSec Tunnel Failover feature.
At least two policies must be configured to use this feature. One policy must be configured as the primary, the other as the secondary.

**Example**
The following command associates the crypto map to a crypto group called `group1` and dictates that it will serve as the primary tunnel policy:

```
match crypto group group1 primary
```
**match ip pool**

Matches the specified IP pool to the current IKEv1 crypto map. This command can be used multiple times to change more than one IP pool.

**Product**
PDSN, HA, GGSN, SCM

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match ip pool pool-name pool_name
no match ip pool pool-name pool_name
```

- **match ip pool pool-name pool_name**
  - `pool_name`
    - The name of an existing IP pool that should be matched.

- **no**
  - Delete the matching statement for the specified IP pool from the crypto map.

**Usage**

Use this command to set the names of IP pools that should be matched in the current crypto map.

---

**Important:** If an IP address pool that is matched to a IKEv1 crypto map is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the `clear crypto` command in the Exec mode for information on clearing security associations.

**Example**

The following command sets a rule for the current crypto map that will match an IP pool named *ippool1*:

```
match ip pool pool-name ippool1
```
set

Configures parameters for the dynamic crypto map.

Product
PDSN, HA, GGSN, SCM

Privilege
Security Administrator, Administrator

Syntax

```plaintext
set { control-dont-fragment ( clear-bit | copy-bit | set-bit ) } | ikev1
    natt [ keepalive time ] | pfs { group1 | group2 | group5 } | phase1-idtype { id-key-id | ipv4-address [ mode { aggressive | main } ] } | phase2-idtype { ipv4-address | ipv4-address-subnet } | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes kbytes | seconds secs } transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]
no set { ikev1 natt | pfs | phase1-idtype | phase2-idtype | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes | seconds } | transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]
```

- **control-dont-fragment ( clear-bit | copy-bit | set-bit )**
  - Controls the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet. Options are:
    - **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
    - **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
    - **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).

- **ikev1 natt [ keepalive time ]**
  - Specifies IKE parameters.
    - **natt**: Enables IPSec NAT Traversal.
    - **keepalive time**: The time to keep the NAT connection alive in seconds. `time` must be an integer of from 1 through 3600 seconds.

- **pfs { group1 | group2 | group5 }**
  - Specifies the modp Oakley group (also known as the Diffie-Hellman (D-H) group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).
    - **group1**: Diffie-Hellman Group 1 (768-bit modp)
    - **group2**: Diffie-Hellman Group 2 (1024-bit modp)
    - **group5**: Diffie-Hellman Group 5 (1536-bit modp)

- **phase1-idtype { id-key-id | ipv4-address [ mode { aggressive | main } ] }**
  - Sets the IKE negotiations Phase 1 payload identifier. Default: id-key-id id-key-id: ID KEY ID
    - **mode**: Configures IKE mode
- aggressive: IKE negotiation mode: AGGRESSIVE
- main: IKE negotiation mode: MAIN

`phase2-idtype { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier. Default: ipv4-address-subnet

`ipv4-address`: Use IPV4_ADDR as the Phase 2 payload identifier.
`ipv4-address-subnet`: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

`security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes kbytes | seconds secs }

Defaults:
- `disable-phase2-rekey`: Rekeying is enabled by default
- `keepalive`: Disabled
- `kilo-bytes`: 4608000 kbytes
- `seconds`: 28800 seconds

This keyword specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.

- `disable-phase2-rekey`: If this keyword is specified, when the lifetime expires, the Phase2 SA is not rekeyed.
- `keepalive`: The SA lifetime expires only when a keepalive message is not responded to by the far end.
- `kilo-bytes`: This specifies the amount of data in kilobytes to allow through the tunnel before the SA lifetime expires. kbytes must be an integer from 2560 through 4294967294.
- `seconds`: The number of seconds to wait before the SA lifetime expires. secs must be an integer from 1200 through 86400.

**Important:** If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map’s SA lifetime (either in terms of kilobytes or seconds), then the `keepalive` parameter must be configured.

`transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]

This keyword specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command `crypto ipsec transform-set` for information on creating transform sets.

You can repeat this keyword up to 6 times on the command line to specify multiple transform sets. `transform_name` is the name of the transform set and must be an alpha and/or numeric string from 1 to 127 characters and is case sensitive.

`no`

Deletes the specified parameter or resets the specified parameter to the default value.

**Usage**

*Cisco ASR 5000 Series Command Line Interface Reference*
Use this command to set parameters for a dynamic crypto map.

**Example**
The following command sets the PFS group to Group1:

```
set pfs group1
```
The following command sets the SA lifetime to 50000 KB:

```
set security-association lifetime kilo-bytes 50000
```
The following command sets the SA lifetime to 10000 seconds:

```
set security-association lifetime seconds 10000
```
The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```
The following command defines transform sets tset1 and tset2.

```
set transform-set tset1 transform-set tset2
```
Chapter 43
Crypto Map IKEv2-IPv6 Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          crypto map name
            ikev2-ipv6
              Crypto Map IKEv2-IPv6 Config Mode
```

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

Configures the subscriber authentication method used for the P-GW lawful intercept service.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```plaintext
authentication pre-shared-key { encrypted key value | key value }
```

**Usage**

Use this command to specify the type of authentication performed for subscribers attempting to access the P-GW service using this crypto map.

**Example**

The following command sets the authentication method to an open key value of 6d7970617373776f7264:

```plaintext
authentication pre-shared-key key 6d7970617373776f7264
```
control-dont-fragment

Controls the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet.

Product
P-GW

Privilege
Administrator

Syntax

control-dont-fragment { clear-bit | copy-bit | set-bit }

{ clear-bit | copy-bit | set-bit }
  clear-bit: Clears the DF bit from the outer IP header (sets it to 0).
  copy-bit: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
  set-bit: Sets the DF bit in the outer IP header (sets it to 1).

Usage
A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example
The following command sets the DF bit in the outer IP header:

  control-dont-fragment set-bit
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Returns to the previous mode.
**ikev2-ikesa**

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```plaintext
ikev2-ikesa ( max-retransmissions number | rekey | setup-timer sec )
default ikev2-ikesa ( max-retransmissions | rekey | setup-timer )
no ikev2-ikesa rekey
```

- **default**
  Restores the selected keyword to its default value.

- **no ikev2-ikesa**
  Disables a previously enabled parameter.

- **max-retransmissions number**
  Default: 5
  Specifies the maximum number of retransmissions of an IKEv2 IKE exchange request if a response has not been received. *number* must be an integer from 1 to 8.

- **rekey**
  Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

- **setup-timer sec**
  Default: 60
  Specifies the number of seconds before a IKEv2 IKE Security Association, that is not fully established, is terminated. *sec* must be an integer from 1 to 3600.

**Usage**

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

**Example**
The following command configures the maximum number of IKEv2 IKESA request retransmissions to 7:

```plaintext
ikev2-ikesa max-retransmissions 7
```
**match**

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
match address acl_name [ priority ]
```

**no match address**

```
no
```

Removes a previously matched ACL.

```
acl_name
```

The name of the ACL that the crypto map is to be matched with. `acl_name` can be from 1 to 79 alpha and/or numeric characters and is case sensitive.

```
priority
```

Default: 0
Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL.
The preference can be configured to any integer value from 0 to 4294967295. “0” is the highest priority.

**Important:** The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

**Usage**

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.
Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

**Example**
The following command sets the crypto map ACL to the ACL named `acl-list1` and sets the crypto maps priority to the highest level.

```
match address acl-list1 0
```
payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

Product
P-GW

Privilege
Administrator

Syntax

```
payload name match ipv6
no payload name
```

**name**
Specifies the name of a new or existing crypto template payload. *name* must be from 1 to 127 alpha and/or numeric characters.

**match ipv6**
Filters IPSec IPv6 Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

**Usage**
Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated. Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the *ip-address-allocation* then no MIP call can be established, just a Simple IP call. Currently, the only available match is for ChildSA, although other matches are planned for future releases. Entering this command results in the following prompt:

```
[<ctxt_name>]hostname(cfg-crypto-<name>-ikev2-tunnel-payload)#
```

Crypto Template IKEv2-IPv6 Payload Configuration Mode commands are defined in the Crypto Template IKEv2-IPv6 Payload Configuration Mode Commands chapter.

**Example**
The following command configures a crypto template payload called *payload5* and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

```
payload payload5 match ipv6
```
peer

Configures the IP address of a peer IPsec server.

Product
P-GW

Privilege
Administrator

Syntax

    peer ip_address

    no peer

    no
    Removes the configured peer server IP address.

    ip_address
    Specifies the IP address of a peer IPsec server. ip_address must be specified in IPv4 dotted decimal notation or IPv6 colon separated notation.

Usage
Use this command to specify a peer IPsec peer server. The IPsec peer server can also be the Lawful Intercept server.

Example
The following command configures the system to recognize an IPsec peer server with an IPv6 address of fe80::200:f8ff:fe21:67cf:

    peer fe80::200:f8ff:fe21:67cf
Chapter 44
Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Payload Configuration Mode is used to assign the correct IPsec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses.
The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax

end

Usage
Change the mode back to the Exec Mode.
exit

Exports the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the previous mode.
ipsec

Configures the IPsec transform set to be used for this crypto template payload.

Product
P-GW

Privilege
Administrator

Syntax

ipsec transform-set list name

no ipsec transform-set list

---

list name

Specifies the context configured IPsec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. name must be from 1 to 127 alpha and/or numeric characters.

---

Usage

Use this command to list the IPsec transform set(s) to use in this crypto template payload.

---

Example

The following command configures IPsec transform sets named ipset1 and ipset2 to be used in this crypto template payload:

ipsec transform-set list ipset1 ipset2
**lifetime**

Configures the number of seconds for IPsec Child SAs derived from this crypto template payload to exist.

**Product**

P-GW

**Privilege**

Administrator

**Syntax**

```
 lifetime sec [ kilobytes kbytes ]
```

```
 default lifetime
```

- **default**
  
  Returns the lifetime value to the default setting of 86400.

- **sec**
  
  Default: 86400
  
  Specifies the number of seconds for IPsec Child Security Associations derived from this crypto template payload to exist. `sec` must be an integer from 60 to 604800.

- **kilobytes kbytes**
  
  Specifies lifetime in kilo-bytes for IPsec Child Security Associations derived from this Crypto Map. `kbytes` must be an integer value from 1 to 2147483648.

**Usage**

Use this command to configure the number of seconds for IPsec Child Security Associations derived from this crypto template payload to exist.

**Example**

The following command configures the IPsec child SA lifetime to be 120 seconds:

```
 lifetime 120
```
rekey

Configures child security association rekeying.

Product
P-GW

Privilege
Administrator

Syntax
rekey [ keepalive ]

[ default | no ] rekey

default
Returns the feature to the default setting of disabled.

no
Disables this feature.

keepalive
If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

Usage
Use this command to enable or disable the ability to rekey IPsec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

Example
The following command disables rekeying:

no rekey
Chapter 45
Crypto Map Manual Configuration Mode Commands

The Crypto Map Manual Configuration Mode is used to configure static IPSec tunnel properties. Modification(s) to an existing crypto map manual configuration will not take effect until the related security association has been cleared. Refer to the clear crypto security-association command located in the Exec Mode Commands chapter of the Command Line Interface Reference for more information.

**Important:** Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be used for testing purposes.

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

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the context configuration mode.
match address

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

**Product**
PDSN, HA, GGSN, PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match address acl_name[priority]
no match address
```

**no**

Removes a previously matched ACL.

**acl_name**
The name of the ACL that the crypto map is to be matched with.

**priority**
Default: 0

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL.

The preference can be configured to any integer value from 0 to 4294967295. “0” is the highest priority.

**Important:** The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

**Usage**

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

**Example**
The following command sets the crypto map ACL to the ACL named **ACLlist1** and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```
set control-dont-fragment

Controls the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet.

Product
PDSN, HA, GGSN, PDIF

Privilege
Security Administrator, Administrator

Syntax

set control-dont-fragment { clear-bit | copy-bit | set-bit }
default set control-dont-fragment { clear-bit | copy-bit | set-bit }

clear-bit
Clears the DF bit from the outer IP header (sets it to 0).

copy-bit
Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

default
Sets / Restores default value assigned to a specified parameter.

set-bit
Sets the DF bit in the outer IP header (sets it to 1).

Usage
Use this command to clear, copy, or set the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet.

Example
The following command sets the DF bit in the outer IP header.

    set control-dont-fragment set-bit
set peer

Configures the IP address of the peer security gateway that the system will establish the IPSec tunnel with.

**Product**
- PDSN, HA, GGSN, PDIF

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
set peer gw_address
no set peer
```

- `no`
  Removes a previously configured peer address.

- `gw_address`
  The IP address of the peer security gateway with which the IPSec tunnel will be established.

**Usage**

Once the manual crypto map is fully configured and applied to an interface, the system will establish an IPsec tunnel with the security gateway specified by this command. Because the tunnel relies on statically configured parameters, once created, it never expires; it exists until its configuration is deleted.

**Example**

The following command configures a security gateway address of 192.168.1.100 for the crypto map to establish a tunnel with.

```
set peer 192.168.1.100
```
set session-key

Configures session key parameters for the manual crypto map.

**Product**
PDSN, HA, GGSN, PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
set session-key { inbound | outbound } { ah ahSpi [ encrypted ] key ah_key
| esp esp_spi [ encrypted ] cipher encryption_key [ encrypted ]
authenticator auth_key }
no set session-key { inbound | outbound }
```

**no**
Removes previously configured session key information.

**inbound**
Specifies that the key(s) will be used for tunnels carrying data sent by the security gateway.

**outbound**
Specifies that the key(s) will be used for tunnels carrying data sent by the system.

**ah ahSpi**
Configures the following session key information for the Authentication Header (AH) protocol:

- **ahSpi**: The security parameter index (SPI) used to identify the AH security association (SA) between the system and the security gateway.
- The SPI can be configured to any integer value from 256 to 4294967295.

**encrypted**
Indicates the key provided is encrypted.

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

**key ah_key**
Configures the following session key information for the Authentication Header (AH) protocol:

- **ah_key**: The key used by the system to de/encapsulate IP packets using the AH protocol.
- The key must be entered as either a string or a hexadecimal number beginning with “0x”.

**esp esp_spi**
Configures security parameter index (SPI) for the Encapsulating Security Payload (ESP) protocol. The SPI is used to identify the ESP security association (SA) between the system and the security gateway.

- **esp_spi**: The SPI value. It can be configured to any integer value from 256 to 4294967295.
crypto map manual configuration mode commands

**set session-key**

cipher encryption_key

Specifies the key used by the system to de/encrypt the payloads of IP packets using the ESP protocol. `encryption_key` must be entered as either a string or a hexadecimal number beginning with “0x”.

authenticator auth_key

Specifies the key used by the system to authenticate the IP packets once encryption has been performed. `auth_key` must be entered as either a string or a hexadecimal number beginning with “0x”.

**Usage**

Manual crypto maps rely on the use of statically configured keys to establish IPSec tunnels. This command allows the configuration of the static keys.

Identical keys must be configured on both the system and the security gateway in order for the tunnel to be established.

This command can be entered up to two times for the same crypto map: once to configure inbound key properties, and once to configure outbound key properties.

**Example**

The following command configures a manual crypto map with the following session key properties:

- Keys are for tunnels initiated by the system to the security gateway.
- ESP will be used with an SPI of 310.
- Encryption key is sd23r9skd0fi3as.
- Authentication key is sfd23408imi9yn.

```
set session-key outbound esp 310 cipher sd23r9skd0fi3as authenticator sfd23408imi9yn
```
**set transform-set**

Configures the name of a transform set that the crypto map is associated with.

**Product**

PDSN, HA, GGSN, PDIF

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
set transform-set transform_name
no set transform-set
```

- `no`
  
  Removes a previously configured transform set association.

  `transform_name`

  Specifies the name of the transform set and must be an alpha and/or numeric string from 1 to 127 characters and is case sensitive.

**Usage**

System transform sets contain the IPSec policy definitions for crypto maps. Refer to the command `crypto ipsec transform-set` for information on creating transform sets.

**Important:** Transform sets must be configured prior to configuring session key information for the crypto map.

**Example**

The following command associates a transform set named `esp_tset` with the crypto map:

```plaintext
set transform-set esp_tset
```
Chapter 46
Crypto Template Configuration Mode Commands

The Crypto Template Configuration Mode is used to configure an IKEv2 IPsec policy. It includes most of the IPsec parameters and IKEv2 parameters for cryptographic and authentication algorithms etc. A security gateway service will not function without a configured crypto template. Only one crypto template can be configured per service.

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

Configures the subscriber authentication method used for the PDIF service.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
authentication { eap-profile name [ second-phase eap-profile name ] | gateway { encrypted key value | key value } | pre-shared-key { encrypted key value | key value } }
```

- **eap-profile name [ second-phase eap-profile name ]**
  Specifies that authentication is to be performed using a named EAP profile. `name` must be from 1 to 127 alpha and/or numeric characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.
  A second-phase eap profile name is only required for installations using multiple authentication. `name` must be from 1 to 127 alpha and/or numeric characters.

- **gateway { encrypted key value | key value }**
  Specifies the pre-shared gateway key used for gateway authentication.
  `encrypted key value`: Specifies that the pre-shared key used for authentication is encrypted. `value` must be between 1 and 255 alpha and/or numeric characters.
  `key value`: Specifies that the pre-shared key used for authentication is clear text. `value` must be between 1 and 255 alpha and/or numeric characters.

- **pre-shared-key { encrypted key value | key value }**
  Specifies that a pre-shared key is to be used for authenticating a subscriber in the service.
  `encrypted key value`: Specifies that the pre-shared key used for authentication is encrypted. `value` must be between 1 and 255 alpha and/or numeric characters.
  `key value`: Specifies that the pre-shared key used for authentication is clear text. `value` must be between 1 and 255 alpha and/or numeric characters.

Usage

Use this command to specify the type of authentication performed for subscribers attempting to access the service using this crypto template.

Entering the `authentication eap-profile` command results in the following prompt:

```
[context_name]hostname(cfg-crypto-tmpl-eap-key)#
```

EAP Authentication Configuration Mode commands are defined in the “EAP Authentication Configuration Mode Commands” chapter.

Example
The following command enables authentication via an EAP profile named `eap23` for subscribers using the service with this crypto template:

```
authentication eap-profile eap23
```
**certificate**

Used to bind an X.509 trusted certificate to a crypto template.

**Product**
- PDIF
- PDG/TTG

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
certificate name name
no certificate
```

```
no
Removes any applied certificate or prevents the certificate from being included in the Auth Exchange response payload.
```

```
name name
An alpha and/or numeric string of 1 - 127 characters.
```

**Usage**

Can be used to bind an X.509 certificate to a template, or include or exclude it from the Auth Exchange response payload.

**Example**

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate
```
control-dont-fragment

Controls the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

control-dont-fragment { clear-bit | copy-bit | set-bit }

Usage
Options are:

- clear-bit: Clears the DF bit from the outer IP header (sets it to 0).
- copy-bit: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- set-bit: Sets the DF bit in the outer IP header (sets it to 1).

Usage
A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example
The following command sets the DF bit in the outer IP header:

```
control-dont-fragment set-bit
```
default

Restores the default values for the selected parameter.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

default { authentication gateway | certificate | dns-handling | dos cookie-challenge detect-dos-attack | ikev2-ikesa { ignore-rekeying-requests | keepalive-user-activity | max-retransmission | mobike | policy error-notification | rekey | retransmission-timeout | setup-timer } | keepalive | nai | natt }

authentication gateway
Configures the default pre-shared gateway key used for authentication.

certificate
Configures the system to remove the certificate for a given crypto template.

dns-handling
Configures the system to use normal dns handling.

dos cookie-challenge detect-dos-attack
Configures the system to disable any Denial of Service attacks.

Ikev2-ikesa { ignore-rekeying-requests | keepalive | max-retransmission | mobike | policy error-notification | rekey | retransmission-timeout | setup-timer }
Configures the system to use the following ikev2-ikesa defaults:
ignore-rekeying-requests: Ignore any IKE_SA rekeying requests received.
keepalive-user-activity: Keepalive messages received from peer will not reset the user inactivity timer.
max-retransmission: Set the number of IKEv2 IKE exchange request retransmissions if the corresponding response has not been received. Default is 5.
mobike. Set MOBIKE to disable.
policy error-notification: Set the default policy error notification method to send error notify messages to the MS.
rekey: Set the default rekeying of IKE_SA to disabled.
retransmission-timeout: Set the maximum number of milliseconds to elapse before an IKEv2 IKE exchange request is retransmitted if the corresponding IKEv2 IKE exchange response has not been received to 500.
setup timer: Set the number of seconds to elapse before a non-fully-established IKEv2 IKE SA is terminated to 60.
**keepalive**
Enable Dead Peer Detection for all SAs derived from this crypto template.

**nai**
Set the default NAI parameters to be used for the crypto template (IDr) to none

**natt**
Enable NAT-T initiation for all SAs derived from this crypto template.

**Usage**
Use these commands to restore default parameters.

**Example**
Use the following command to disable MOBIKE by default:
```
default mobike
```
**dns-handling**

Adds a custom option to define the ways a DNS address is returned based on proscribed circumstances described below.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default ] dns-handling { normal | custom }
```

**default**

Configures the default condition as **normal**. By default, PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

**normal**

This is the default action. PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

**custom**

Configures the PDIF to behave as described in the Usage section below.

**Usage**

During IKEv2 session setup, MS may or may not include INTERNAL_IP4_DNS in the Config Payload (CP). PDIF may obtain one or more DNS addresses for the subscriber in DNS NVSE from a proxy-MIP Registration Reply message. If Multiple Authentication is used, these DNS addresses may be also received in Diameter AVPs during the first authentication phase, or in RADIUS attributes in the Access Accept messages during the second authentication phase.

In **normal** mode, by default PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

In **custom** mode, depending on the number of INTERNAL_IP4_DNS, PDIF supports the following behaviors:

- If MS includes no INTERNAL_IP4_DNS in Config Payload: PDIF doesn't return any INTERNAL_IP4_DNS option to MS, whether or not PDIF has received one(s) in DNS NVSE from HA or from local configurations.
- If MS requests one or more INTERNAL_IP4_DNS(s) in Config Payload, and if P-MIP NVSE doesn't contain any DNS address or DNS address not present in any config, PDIF omits INTERNAL_IP4_DNS option to MS in the Config Payload.
- And if P-MIP NVSE includes one DNS address (a.a.a.a / 0.0.0.0), then PDIF sends one INTERNAL_IP4_DNS option in Config Payload back to the MS.
- If Primary DNS is a.a.a.a and Secondary DNS is 0.0.0.0, then a.a.a.a is returned (i.e. only one instance of DNS attribute present in the config payload).
• If Primary DNS is 0.0.0.0 and Secondary DNS is a.a.a.a, then a.a.a.a is returned (i.e. only one instance of DNS attribute present in the config payload). PDIF does not take 0.0.0.0 as a valid DNS address that can be assigned to the MS.

• And if P-MIP NVSE includes two DNS addresses (a.a.a.a and b.b.b.b) or configurations exists for these two addresses, then PDIF sends two INTERNAL_IP4_DNSs in the CP for the MS (typically known as primary and secondary DNS addresses).

Example
The following configuration applies the custom dns-handling mode:

dns-handling custom
**dos cookie-challenge notify-payload**

Configure the cookie challenge params for IKEv2 INFO Exchange notify payloads for the given crypto template.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

dos cookie-challenge notify-payload [ half-open-sess-count { start integer | stop integer } ] default cookie-challenge detect-dos-attack

no cookie-challenge detect-dos-attack

**Usage**

The following example configures the cookie challenge to begin when the half-open-sess-count reaches 50000 and stops when it drops below 20000:

```
no
```

**Example**

This feature (which is disabled by default) helps prevent malicious Denial of Service attacks against the server by sending a challenge cookie. If the response from the sender does not incorporate the expected cookie data, the packets are dropped.
dos cookie-challenge notify-payload half-open-sess-count start 50000 stop 20000
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Returns to the previous mode.
ikeyv2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

**Product**

PDIF
PDG/TTG

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
ikeyv2-ikesa { keepalive-user-activity | max-retransmissions number | retransmission-timeout msec | policy error-notification [ invalid-message-id | invalid-syntax ] rekey | setup-timer sec | transform-set list name }

default ikeyv2-ikesa { max-retransmissions | policy error-notification [ invalid-message-id | invalid-syntax ] rekey | retransmission-timeout | setup-timer }

no ikeyv2-ikesa { keepalive-user-activity | list name | policy error-notification [ invalid-message-id | invalid-syntax ] | rekey }
```

**no ikeyv2-ikesa**

Disables a previously enabled parameter.

**keepalive-user-activity**

Default is no keepalive-user-activity. Activate to reset the user inactivity timer when keepalive messages are received from peer.

**max-retransmissions number**

Default: 5

Specifies the maximum number of retransmissions of an IKEv2 IKE exchange request if a response has not been received. `number` must be an integer from 1 to 8.

**policy error-notification**

Default is to enable. Default policy is to generate an IKEv2 Invalid Message ID error when PDIF receives an out-of-sequence packet.

**retransmission-timeout msec**

Default: 500

Specifies the timeout period in milliseconds before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received). `msec` must be an integer from 300 to 15000.

**rekey**

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.
setup-timer sec
Default: 16
Specifies the number of seconds before a IKEv2 IKE Security Association, that is not fully established, is terminated. sec must be an integer from 1 to 3600.

transform-set list name
Specifies the name of context-level configured IKEv2 IKE Security Association transform set. name must be an existing IKEv2 IKESA Transform Set and be from 1 to 127 alpha and/or numeric characters.

default
A space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

Usage
Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example
The following command configures the maximum number of IKEv2 IKESA request retransmissions to 7:

ikev2-ikesa max-retransmissions 7

The following command configures the IKEv2 IKESA request retransmission timeout to 400:

ikev2-ikesa retransmission-timeout 400

The following command configures the IKEv2 IKESA transform set list name to ikesa43:

ikev2-ikesa transform-set list ikesa43
keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
keepalive [ interval sec ] [ timeout sec ] [ num-retry num ]
default keepalive [ interval ] [ timeout ] [ num-retry ]
no keepalive
```

- **no**
  Disables keepalive messaging.

- **interval sec**
  Default: 10
  Specifies the amount of time in seconds that must elapse before the next keepalive request is sent. `sec` must be an integer from 10 to 3600.

- **timeout sec**
  Default: 10
  Specifies the amount of time in seconds that the system will wait without receiving a reply before retrying the keepalive request. `sec` must be an integer from 10 to 3600.

- **num-retry num**
  Default: 2
  Specifies the number of times the system will retry a non-responsive peer before defining the peer as off-line or out-of-service. `num` must be an integer from 1 to 100.

**Usage**

Use this command to set parameters associated with determining the availability of peer servers.

**Example**
The following command sets a keepalive interval to three minutes, the timeout to 30 seconds, and the retry attempts number to 5:

```
keepalive interval 180 timeout 30 num-retry 5
```
nai

Configures the NAI parameters to be used for the crypto template IDr.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

[ default | no ] nai idr name id-type { rfc822-addr | fqdn | ip-addr | key-id } 

Default
Configures the default command no nai idr. As a result, the default behavior is for the PDIF-service IP address to be sent as the IDr value of type ID_IP_ADDR.

no

no nai idr configures the value whereby the PDIF service IP address is sent as the IDr value with the type ID_IP_ADDR. This is the default condition.

idr name

name is a string of up to 79 alpha and/or numeric characters.

id-type { rfc822-addr | fqdn | ip-addr | key-id }

Configures the NAI IDr id-type parameter. If no id-type is specified, then rfc822-addr is assumed.

rfc822-addr configures NAI Type ID_RFC822_ADDR

fqdn configures NAI Type ID_FQDN

ip-addr configures NAI Type ID_IP_ADDR

key-id configures NAI Type ID_KEY_ID

Usage

The configured IDr is sent from the PDIF to the MS in the first IKEv2 AUTH response.

Example

The following command configures the NAI IDr to the default condition.

no nai idr
**natt**

Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] natt [ send-keepalive ]
```

**no**
Disables NAT-T for all security associations associated with this crypto template.

**send-keepalive**
Sends NAT-Traversal keepalive messages.

**Usage**
Use this command to configure NAT-T for security associations within this crypto template.

**Example**
The following command disables NAT-T for this crypto template:

```
no natt
```
payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
payload name match childsa [ match { ipv4 | ipv6 } ]
```

```
no payload name
```

- **name**
  Specifies the name of a new or existing crypto template payload. `name` must be from 1 to 127 alpha and/or numeric characters.

- **match childsa [ match { ipv4 | ipv6 } ]**
  Filters IPSec Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:
  - `ipv4`: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4.
  - `ipv6`: Configures this payload to be applicable to IPSec Child Security Association requests for IPv6.

**Usage**

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.

Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the `ip-address-allocation` then no MIP call can be established, just a Simple IP call.

Currently, the only available match is for ChildSA, although other matches are planned for future releases.

Omitting the second match parameter for either IPv4 or IPv6 will make the payload applicable to all IP address pools.

Entering this command results in the following prompt:

```
[cfg-crypto tmpl-ikev2-tunnel-payload]#
```

Crypto Template Payload Configuration Mode commands are defined in the Crypto Template Payload Configuration Mode Commands chapter.

**Example**

The following command configures a crypto template payload called `payload5` and enters the Crypto Template Payload Configuration Mode:

```
payload payload5 match childsa
```
Chapter 47
Crypto Template IKEv2-PDIF Payload Configuration Mode Commands

The Crypto Template IKEv2-PDIF Payload Configuration Mode is used to assign the correct IPsec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme as this is how the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for ip-address-allocation.
Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**default**

Sets or restores the default value for the specified parameter.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default { ignore-rekeying-requests | ip-address-allocation lifetime | maximum-child-sa | rekey | tsi | tsr }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ignore-rekeying-requests</strong></td>
<td>Configures the system to ignore IPSec SA rekey requests.</td>
</tr>
<tr>
<td><strong>ip-address-allocation</strong></td>
<td>Configures the crypto map payload IP address allocation scheme to be the home address.</td>
</tr>
<tr>
<td><strong>lifetime</strong></td>
<td>Configures the default lifetime for IPSec Child SAs derived from this crypto template. lifetime: 86400 seconds.</td>
</tr>
<tr>
<td><strong>maximum-child-sa</strong></td>
<td>Configures the maximum number of IPSec Child SAs to be derived from an IKEv2 IKE SA by default. maximum-child-sa: 1</td>
</tr>
<tr>
<td><strong>rekey</strong></td>
<td>Configures the system to disable Child SA rekeying.</td>
</tr>
<tr>
<td><strong>tsi</strong></td>
<td>Configures the default TSi payload to be that of the mobile endpoint.</td>
</tr>
<tr>
<td><strong>tsr</strong></td>
<td>Configures the default IKEv2 Responder Traffic Selector payload options.</td>
</tr>
</tbody>
</table>

**Usage**

Configures system defaults

**Example**

Use the following configuration to set the TSi payload start-address to be that of the Mobile endpoint:

```
default tsi
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

   end

Usage
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Returns to the previous mode.
ignore-rekeying-requests

Ignores CHILD SA rekey requests from the PDIF.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ignore-rekeying-requests
```

**Usage**

Prevents creation of a CHILD SA based on this crypto template.
ip-address-allocation

Configures IP address allocation for subscribers using this crypto template payload. Configure two payloads per crypto template. The first must have a dynamic address to assign a TIA to the ChildSA. The second payload is configured after a successful MIP initiation and can use the default HoA option.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

- `ip-address-allocation { dynamic | home-address | static }
- default ip-address-allocation`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dynamic</strong></td>
<td>Specifies that the IP address for the subscriber is allocated from a dynamic IP pool.</td>
</tr>
<tr>
<td><strong>home-address</strong></td>
<td>Specifies that the IP address for the subscriber is allocated by the Home Agent. This is the default setting for this command.</td>
</tr>
<tr>
<td><strong>static</strong></td>
<td>Specifies that the IP address for the subscriber is a static simple IP address.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure how ChildSA payloads are allocated IP addresses for this crypto template.

**Example**
The following command is for the first ChildSA and will ensure that it gets a TIA address from an IP address pool:

```
ip-address-allocation dynamic
```

The following command is for the second ChildSA and will ensure that it gets a HoA address from the HA:

```
default ip-address-allocation
```
ipsec

Configures the IPsec transform set to be used for this crypto template payload.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
ipsec transform-set list name
no ipsec transform-set list
```

```
list name
```

Specifies the context configured IPsec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. `name` must be from 1 to 127 alpha and/or numeric characters.

Usage
Use this command to list the IPsec transform set(s) to use in this crypto template payload.

Example
The following command configures IPsec transform sets named `ipset1` and `ipset2` to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```
**lifetime**

Configures the number of seconds for IPsec Child SAs derived from this crypto template payload to exist.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
lifetime sec
```

```Syntax
default lifetime

- **sec**
  Default: 86400
  Specifies the number of seconds for IPsec Child Security Associations derived from this crypto template payload to exist. `sec` must be an integer from 60 to 86400.

**Usage**

Use this command to configure the number of seconds for IPsec Child Security Associations derived from this crypto template payload to exist.

**Example**

The following command configures the IPsec child SA lifetime to be 120 seconds:

```
lifetime 120
```
maximum-child-sa

Encrypts the maximum number of IPsec child security associations that can be derived from a single IKEv2 IKE security association.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax
maximum-child-sa num
default maximum-child-sa

num
Default: 1
Specifies the maximum number of IPsec child security associations that can be derived from a single IKEv2 IKE security association. num must be 1.

Usage
Use this command to configure the maximum number of IPsec child security associations that can be derived from a single IKEv2 IKE security association.

Example
The following command configures the maximum number of child SAs to 1:

    maximum-child-sa 1
rekey

Configures Child security association rekeying.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

[ no ] rekey [ keepalive ]

no
Disables this feature.

keepalive
If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

Usage
Use this command to enable or disable the ability to rekey IPsec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

Example
The following command disables rekeying:

    no rekey
tsi

Configures the IKEv2 Initiator Traffic Selector (TSI) payload address options.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
ts start-address { any { end-address any } | endpoint { end-address endpoint } }
```

```
any { end-address any }
```

Configures the TSi payload to allow all IP addresses.

```
endpoint { end-address endpoint }
```

Configures the TSi payload start-address to be that of the Mobile endpoint. This is the default value. `endpoint` is the mobile endpoint netmask.

Usage
On receiving a successful IKE_SA_INIT Response from PDIF, the MS sends an IKE_AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it includes the MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes an IDi payload containing the NAI, SA, TSi, TSr, and CP (requesting IP address and DNS address) payloads.

Example
Use the following example to configure a TSi payload that allows all addresses:

```
ts start-address any end-address any
```
tsr

Configures the IKEv2 Responder Traffic Selector (TSr) payload address options.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Syntax

```tsr start-address <ipv4 address> end-address <ipv4 address>```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-address</td>
<td>Configures the TSi payload to include the TSr start IPv4 address of an address range for the Phase 1 multiple traffic selector feature.</td>
</tr>
<tr>
<td>end-address</td>
<td>Configures the TSi payload start-address to include the TSr end IPv4 address of an address range for the Phase 1 multiple traffic selector feature.</td>
</tr>
</tbody>
</table>

Usage
As part of Phase 1 of the Multiple Traffic Selector feature, this command is used to specify an IPv4 address range in the single TSr payload that the PDG/TTG returns in the last IKE_AUTH message. This TSr is Child SA-specific.

Example
Use the following example to configure a TSr payload that specifies an IPv4 address range for the payload:

```tsr start-address <ipv4 address> end-address <ipv4 address>```
Chapter 48
Crypto Transform Set Configuration Mode Commands

The Crypto Transform Set Configuration Mode is used to configure properties for system transform sets. Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dep
```

**Usage**
Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the context configuration mode.
mode

Configures the IPSec encapsulation mode.

Product
PDSN, HA, GGSN, PDIF, SCM

Privilege
Security Administrator, Administrator

Syntax
mode { transport | tunnel }

transport
Default: Disabled
Specifies that the transform set only protects the upper layer protocol data portions of an IP datagram, leaving the IP header information unprotected.

Important: This mode should only be used if the communications end-point is also the cryptographic end-point.

Default: Enabled
Specifies that the transform set protects the entire IP datagram as displayed in the following figure. This mode should be used if the communications end-point is different from the cryptographic end-point as in a VPN.

Usage
This command specifies the encapsulation mode for the transform set.

Example
The following command configures the transforms set’s encapsulation mode to transport:

mode transport
Chapter 49
CSCF Access Profile Configuration Mode Commands

The Access Profile Configuration Mode is used to set commands supporting the use of signaling compression, authentication, and SIP timers for subscribers accessing the system from varying network types.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

cscf access-profile { default | name name }

Access Profile Configuration Mode
```

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

Sets the type of access security for a P-CSCF/A-BG.

Product  
SCM (P-CSCF, A-BG)

Privilege  
Administrator

Syntax

[ no ] access-security-type ipsec-3gpp-cscf

no
Disables the selected access security type.

ipsec-3gpp-cscf
Security mechanism 3GPP/3GPP2 IPSec.

Usage

Use this command to enable or disable an access security type for a P-CSCF or A-BG.

Example

Enables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:

access-security-type ipsec-3gpp-cscf

Disables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:

no access-security-type ipsec-3gpp-cscf
authentication

Sets the authentication method to use for subscribers using this access profile.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
[ no ] authentication { aka-v1 | md5 }
```

- **no**
  - Disables the selected authentication type.

- **aka-v1 | md5**
  - **aka-v1**: Specifies that the AKA-v1 algorithm will be used for subscribers using this access profile.
  - **md5**: Specifies that the MD5 algorithm will be used for subscribers using this access profile. This is the default setting for this command.

Usage
Use this command to set the authentication method used for subscribers using this access profile.

Example
The following command sets the authentication type for subscribers using this access profile to **md5**:

```
authentication md5
```
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
- All

**Privilege**
- Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

```
exit
```

Usage
Return to the previous mode.
sigcomp

Enables signalling compression for the Access Profile.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

[ no ] sigcomp [ force ]

---

no

Disables signalling compression for the Access Profile.

---

force

Specifies that signaling compression is to be forced for the access type. When this feature is enabled, messages received by the P-CSCF/A-BG that are not compressed are rejected.

---

Usage

Use this command to enable signalling compression for the specific Access Profile.
timeout

Sets timeout values for CSCF and SIP transactions for subscribers using this Access Profile.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
timeout sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | d sec | invite-expiry sec | t1 msec | t2 sec | t4 sec }

default timeout sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | d | invite-expiry | t1 | t2 | t4 }
```

Sets transaction and expiry timers for SIP.

3gpp-d sec: This time is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport. 

Default: 64*T1 (128 seconds, recommended minimum)

3gpp-t1 msec: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport.

Default: 2000 ms (2 secs, recommended minimum).

3gpp-t2 sec: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport.

Default: 16 seconds (recommended minimum).

3gpp-t4 sec: This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport.

Default: 17 seconds (recommended minimum).

d sec: This time is used to control the retransmission of 200OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport.

Default: 64*T1 (32 seconds, recommended minimum)

invite-expiry sec: This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport.

Default: 100 seconds (recommended minimum).

t1 msec: Specifies the time interval (in milliseconds) between each retransmission. The interval doubles after each retransmission, for example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport.
### Usage

Use this command to configure SIP Stack timers and CSCF service specific timers for subscriber traffic using this Access Profile.

### Example

The following command sets the SIP d timer to 64 seconds:

```
timeout sip d 64
```
Chapter 50
CSCF ACL Configuration Mode Commands

The CSCF ACL (Access Control List) Configuration Mode is used to configure session permissions (permit/deny access) within the system.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          cscf acl
            { default | name list_name }
              ACL Configuration Mode
```

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

Places the CSCF ACL entry at the bottom or end of the ACL. Use this command in conjunction with the `permit` and/or `deny` commands.

**Product**
SCM

**Privilege**
Administrator

**Syntax**
```
after
```

**Usage**
Add this command before the `permit` and/or `deny` commands to place the entry at the end of the ACL.
before

Places the CSCF ACL entry at the beginning or top of the ACL. Use this command in conjunction with the `permit` and/or `deny` commands.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
before
```

**Usage**
Add this command before the `permit` and/or `deny` commands to place the entry at the beginning of the ACL.
deny

Configures the system to deny subscriber sessions based on criteria matching the received packet.

Product
SCM

Privilege
Administrator

Syntax

deny { any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | source { address ip_address | aor aor } }

no deny { any | destination aor aor | source { address ip_address | aor aor } }

| any |
| Filters all CSCF sessions. |

| destination aor aor |
| Filters sessions based on the destination AoR. aor must be an existing AoR from 1 to 79 characters in length. |

**Important:** AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

| log { any | destination aor aor | source { address ip_address | aor aor } } |
| Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility acl-log` command in the Exec mode. |

**Specifies the criteria that packets will be compared against. The following criteria is supported:**

- any
- destination aor aor
- source address ip_address
- source aor aor

| source { address ip_address | aor aor } |
| Filters session based on the source IP address or AoR. |

- `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- `aor` must be an existing AoR from 1 to 79 characters in length.

**Important:** AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.
**deny**

```plaintext
no deny { any | destination aor aor | source { address ip_address | aor aor } }
```

Removes specified filter criteria.

**Usage**

Specifies the subscriber sessions to deny based on the criteria specified.

**Example**

The following command denies access to subscribers with a source address of 1.2.3.4:

```plaintext
deny source address 1.2.3.4
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

exit

Usage
Return to the previous mode.
permit

Configures the system to allow subscriber sessions based on criteria matching the received packet.

Product
SCM

Privilege
Administrator

Syntax

```
permit { any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | source { address ip_address | aor aor } }

no permit { any | destination aor aor | source { address ip_address | aor aor } }
```

- **any**
  Filters all CSCF sessions.

- **destination aor aor**
  Filters sessions based on the destination AoR.
  *aor* must be an existing AoR from 1 to 79 characters in length.

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **log { any | destination aor aor | source { address ip_address | aor aor }**
  Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility acl-log` command in the Exec mode.
  Specifies the criteria that packets will be compared against. The following criteria is supported:
  - *any*
  - *destination aor aor*
  - *source address ip_address*
  - *source aor aor*

- **source { address ip_address | aor aor }**
  Filters session based on the source IP address or AoR.
  - *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
  - *aor* must be an existing AoR from 1 to 79 characters in length.

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.
no permit { any | destination aor aor | source { address ip_address | aor aor } }

Removes specified filter criteria.

**Usage**

Specifies the subscriber sessions to permit based on the criteria specified.

**Example**
The following command permits access to subscribers with a destination AoR of $.abc123.com

```
permit destination aor $.abc123.com
```
Chapter 51
CSCF AoR Policy Rules Configuration Mode Commands

The CSCF AoR Policy Rules Configuration Mode is used to manage AoR policy profiles within the system. Both default and user-defined profiles can be managed in this mode.

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

Places the CSCF policy entry at the bottom or end of the policy list. Use this command in conjunction with the `aor` command.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
after
```

**Usage**

Add this command before the `aor` command to place the entry at the end of the policy list.
**aor**

Configures an AoR profile and enters the AoR Profile Configuration Mode.

**Product**

SCM

**Privilege**

Administrator

**Syntax**

```
[ no ] aor aor_name
```

no

Removes the AoR profile from the system.

aor_name

Specifies a name for the AoR profile.

*aor_name* must be from 1 to 79 alpha and/or numeric characters in length.

**Usage**

Use this command to create or modify an AoR profile and enter the CSCF Policy Rules Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-aor_name-aor)#
```

CSCF Policy Rules Configuration Mode commands are defined in the CSCFPolicy Rules Configuration Mode Commands chapter of this guide.

**Example**

The following command creates an AoR profile named *aor5* and enters the AoR Profile Configuration Mode:

```
aor aor5
```
before

Places the CSCF policy entry at the top or beginning of the policy list. Use this command in conjunction with the `aor` command.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```plaintext
before
```

**Usage**
Add this command before the `aor` command to place the entry at the beginning of the policy list.
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
Chapter 52
CSCF Charging Configuration Mode Commands

The CSCF Charging Configuration Mode is used to manage CSCF service policy profiles within the system.

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

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
`end`

Usage
Change the mode back to the Exec mode.
exclude

Configures the service to exclude SIP requests from the Rf charging configuration.

Product
SCM

Privilege
Administrator

Syntax

[ no ] exclude { custom sip_method | invite | notify | register | subscribe | update | message }

- **no**
  Removes the exclusion of the specified SIP request message type.

- **custom sip_method**
  Specifies CUSTOM SIP requests that are to be excluded from Rf charging.
  sip_method can be a name of any SIP method and be from 1 to 31 alpha and/or numeric characters.

- **invite**
  Specifies that INVITE SIP requests are to be excluded from Rf charging.

- **notify**
  Specifies that NOTIFY SIP requests are to be excluded from Rf charging.

- **register**
  Specifies that REGISTER SIP requests are to be excluded from Rf charging.

- **subscribe**
  Specifies that SUBSCRIBE SIP requests are to be excluded from Rf charging.

- **update**
  Specifies that UPDATE SIP requests are to be excluded from Rf charging.

- **message**
  Specifies that MESSAGE SIP requests are to be excluded from Rf charging.

Usage
Use this command to exclude specific SIP requests from Rf charging.

Example
The following command configures the service to exclude SIP REGISTER requests from Rf charging:
exclude register
exit

Exits the current mode and returns to the previous mode.

**Product**  All

**Privilege**  Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
Chapter 53
CSCF Crypto Template Configuration Mode Commands

The CSCF Crypto Template Configuration Mode is used to configure a P-CSCF IPsec policy. It includes most of the IPsec parameters and Internet Key Exchange version 1 (IKEv1) parameters for cryptographic and authentication algorithms etc. A P-CSCF service will not support IPsec without a configured crypto template. Only one crypto template can be configured per P-CSCF service.

```
Exec Mode
  configure
  Global Configuration Mode
    context name
    Context Configuration Mode
      crypto template name ipsec-3gpp-cscf
      CSCF Crypto Template Configuration Mode
```

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

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage

Returns to the previous mode.
ipsec

Configures parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

Product
SCM

Privilege
Security Administrator, Administrator

Syntax

```
ipsec transform-set list list_name
```

```
transform-set list name

transform-set: Specifies a context-level IPSec security association transform set to be used for deriving 3GPP/3GPP2 P-CSCF security associations from this crypto template.
lst list_name: A space separated list of 3GPP/3GPP2 P-CSCF security association transform sets. list_name must be an existing 3GPP/3GPP2 P-CSCF transform set and be from 1 to 127 alpha and/or numeric characters.
```

⚠️ Important: A minimum of one transform set is required. A maximum of four transform sets may be specified.

Usage

Use this command to configure parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

Example

The following command configures the 3GPP/3GPP2 P-CSCF transform set list name to `ikev1list1`:

```
ipsec transform-set list ikev1list1
```
Chapter 54
CSCF Emergency-CSCF Configuration Mode Commands

The Emergency-CSCF Configuration Mode is used to set commands supporting the role of the CSCF service as an Emergency CSCF.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

cscf service name

CSCF Service Configuration Mode

emergency-cscf

Emergency-CSCF Configuration Mode
```

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

Exits the current mode and returns to the Exec Mode.

**Product**

All

**Privilege**

Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

exit

Usage

Return to the previous mode.
privacy

Enables privacy support on the E-CSCF.

Product
SCM

Privilege
Administrator

Syntax

privacy

[ no | default ] privacy

Usage

Use this command to enable privacy support for Emergency CSCF service.
The CSCF Enforce Codec Policy Configuration Mode is used to manage audio and video codec policies within the system. The parameters defined in this chapter are derived from IETF RFC 3551: “RTP Profile for Audio and Video Conferences with Minimal Control”.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

cscf policy { default | name policy_name }

CSCF Policy Configuration Mode

aor-policy-rules

AoR Policy Configuration Mode

CSCF Policy Rules Config Mode

service-policy-rules

enforce-codec-policy

Enforce Codec Policy Config Mode

aor name

CSCF Policy Rules Config Mode
```
**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**dynamic-codec**

Creates a list of dynamic codecs supported by the system.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
dynamic-codec { audio encoding_name | video encoding_name } [ clock_rate ] [ channels ]
```

```
default dynamic-codec
```

```
no dynamic-codec [ encoding_name ] [ clock_rate ] [ channels ]
```

- **audio encoding_name | video encoding_name**
  - audio `<encoding_name>`: Specifies the encoding name of the dynamic audio codec added to the allowed codec list. `<encoding_name>` must be from 1 to 49 alpha and/or numeric characters.
  - video `<encoding_name>`: Specifies the encoding name of the dynamic video or audio-video codec added to the allowed codec list. `<encoding_name>` must be from 1 to 49 alpha and/or numeric characters.

- **[ clock_rate ] [ channels ]**
  - `clock_rate`: Specifies the sampling rate of the codec. `clock_rate` must be an integer from 0 to 1000000.
  - `channels`: Specifies the number of channels required by the codec. `channels` must be an integer from 1 to 1000000.

**Valid dynamic audio codecs:**

<table>
<thead>
<tr>
<th>Encoding Name</th>
<th>Clock Rate (Hz)</th>
<th>Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>G726-40</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-32</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-24</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-16</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G729D</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G729E</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>GSM-EFR</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>L8</td>
<td>Variable</td>
<td></td>
</tr>
<tr>
<td>RED</td>
<td>See RFC3551</td>
<td></td>
</tr>
<tr>
<td>VDVI</td>
<td>Variable</td>
<td>1</td>
</tr>
</tbody>
</table>

**Valid dynamic video codecs:**
### dynamic-codec

<table>
<thead>
<tr>
<th>Encoding Name</th>
<th>Clock Rate (Hz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H263-1998</td>
<td>90,000</td>
</tr>
</tbody>
</table>

#### default

Specifies that the default list of dynamic codecs is added to the allowed codecs list. Default dynamic codecs: H263 and AMR.

```
default
```

#### no dynamic-codec [ encoding_name ] [ clock_rate ] [ channels ]

Specifies that all dynamic codecs are removed from the allowed codecs list. If an encoding_name is specified, then only the codec specified by the encoding_name is removed. Furthermore, if a supporting clock_rate and/or channels are specified, then only the encoding_name with the specified clock_rate and/or channels is removed.

```
no dynamic-codec
```

#### Usage

Use this commands to create a list of supported dynamic audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

#### Example

The following command adds the GSM-EFR codec to the allowed dynamic codec list:

```
dynamic-codec GSM-EFR
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax

end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**

All

**Privilege**

Administrator

**Syntax**

`exit`

**Usage**

Return to the previous mode.
**static-codec**

Creates a list of static codecs supported by the system.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
static-codec { audio payload_type | video payload_type }

default static-codec

no static-codec [ payload_type ]
```

**audio payload_type | video payload_type**

*audio payload_type*: Specifies the audio codec added to the allowed codecs list. *payload_type* must be an integer from 0 to 95. Default value is 5.

**Valid static audio codecs**:

<table>
<thead>
<tr>
<th>Audio Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: PCMU</td>
<td></td>
</tr>
<tr>
<td>1: reserved</td>
<td></td>
</tr>
<tr>
<td>2: reserved</td>
<td></td>
</tr>
<tr>
<td>3: GSM</td>
<td></td>
</tr>
<tr>
<td>4: G723</td>
<td></td>
</tr>
<tr>
<td>5: DVI4</td>
<td></td>
</tr>
<tr>
<td>6: DVI4</td>
<td></td>
</tr>
<tr>
<td>7: LPC</td>
<td></td>
</tr>
<tr>
<td>8: PCMA</td>
<td></td>
</tr>
<tr>
<td>9: reserved</td>
<td></td>
</tr>
<tr>
<td>10: L16</td>
<td></td>
</tr>
<tr>
<td>11: L16</td>
<td></td>
</tr>
<tr>
<td>12: QCELP</td>
<td></td>
</tr>
<tr>
<td>13: CN</td>
<td></td>
</tr>
<tr>
<td>14: MPA</td>
<td></td>
</tr>
<tr>
<td>15: G728</td>
<td></td>
</tr>
<tr>
<td>16: DVI4</td>
<td></td>
</tr>
<tr>
<td>17: DVI4</td>
<td></td>
</tr>
<tr>
<td>18: G729</td>
<td></td>
</tr>
<tr>
<td>19: reserved</td>
<td></td>
</tr>
<tr>
<td>20: unassigned</td>
<td></td>
</tr>
<tr>
<td>21: unassigned</td>
<td></td>
</tr>
<tr>
<td>22: unassigned</td>
<td></td>
</tr>
</tbody>
</table>

*video payload_type*: Specifies the video or audio-video codec added to the allowed codecs list. *payload_type* must be an integer from 0 to 95. Default value is 5.

**Valid static video codecs**:

<table>
<thead>
<tr>
<th>Video Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24: unassigned</td>
<td></td>
</tr>
<tr>
<td>25: CelB</td>
<td></td>
</tr>
<tr>
<td>26: JPEG</td>
<td></td>
</tr>
<tr>
<td>27: unassigned</td>
<td></td>
</tr>
<tr>
<td>28: nv</td>
<td></td>
</tr>
<tr>
<td>29: unassigned</td>
<td></td>
</tr>
<tr>
<td>30: unassigned</td>
<td></td>
</tr>
<tr>
<td>31: H261</td>
<td></td>
</tr>
<tr>
<td>32: MPV</td>
<td></td>
</tr>
<tr>
<td>33: MP2T</td>
<td></td>
</tr>
<tr>
<td>34: H263</td>
<td></td>
</tr>
<tr>
<td>35-71: unassigned</td>
<td></td>
</tr>
<tr>
<td>72-76: reserved</td>
<td></td>
</tr>
<tr>
<td>77-95: unassigned</td>
<td></td>
</tr>
</tbody>
</table>

**default**

Specifies that the default list of static codecs is added to the allowed codecs list. The default static codec is 5: DVI4.
static-codec

**no static-codec [ payload_type ]**

Specifies that all static codecs are removed from the allowed codecs list. If a `payload_type` is specified, then only the codec specified by the `payload_type` is removed.

**Usage**

Use this command to create a list of supported static audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

**Example**

The following command adds the G729 audio codec to the allowed codecs list:

```
static-codec 18
```
Chapter 56
CSCF IFC SPT Group Mode Commands

The CSCF iFC SPT Group Configuration Mode is used to associate individual SPT conditions with an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

cscf ifc-spt-group name name

IFC SPT Group Configuration Mode
```

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

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```plaintext
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
spt-condition

Assigns iFC SPT conditions to an existing iFC SPT group.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

```plaintext
[ no ] spt-condition name cond_name
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified CSCF iFC SPT condition from the iFC SPT group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>spt-condition name cond_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of an existing iFC SPT condition.</td>
</tr>
<tr>
<td><code>cond_name</code> must be from 1 to 39 alpha and/or numeric characters in length.</td>
</tr>
</tbody>
</table>

Usage
Use this command to associate individual SPT conditions with an iFC SPT group.

**Important:** An iFC SPT group may be associated with multiple SPT conditions.

Example
The following command assigns cond2 to an iFC SPT group:

```plaintext
spt-condition name cond2
```
Chapter 57
CSCF IFC Trigger Point Mode Commands

The CSCF iFC Trigger Point Configuration Mode is used to associate an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group with an iFC trigger point.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          cscf ifc-trigger-point
            name name
            condition-type { cnf | dnf }
              IFC Trigger Point Configuration Mode
```

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

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
spt-group

Assigns an existing iFC SPT group to an iFC trigger point.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

[ no ] spt-group name group_name

no
Removes the specified CSCF iFC SPT group from the iFC trigger point.

spt-group name group_name
Specifies the name of an existing iFC SPT group.

Important: An iFC SPT group can be assigned to more than one iFC trigger point.

Usage
Use this command to associate an iFC SPT group with an iFC trigger point.

Example
The following command assigns an iFC SPT group named group2 to an iFC trigger point:

spt-group name group2
Chapter 58
CSCF ISC Template Configuration Mode Commands

The CSCF ISC Template Configuration Mode is used to configure the IMS Service Control (ISC) interface within the system.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          cscf isc-template name name
            ISC Template Configuration Mode
```

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

Core Network Service Authorization (CNSA) related commands used to create media profile and service ids.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

```cnsa { media-profile-id profile_id | service-id service_id [ service_id ]...[ service_id ] }
```

```no cnsa { media-profile-id | service-id [ service_id ] [ service_id ]...[ service_id ] }
```

### media-profile profile_id

Specifies the cnsa media profile id.

- `profile_id` must be an integer from 0 to 10.
- The media profile id is assigned to a service policy using the **cnsa-media-profile** command under CSCF Service configuration.

### Important:
You can only create one media profile id per ISC template.

### service-id service_id

Specifies the cnsa service id(s). These ids represent URN parameters which are ICSI (IMS Communication Service Identifier) values that are mapped to a service profile through a media profile id.

- `service_id` must be from 1 to 79 alpha and/or numeric characters.

```no cnsa { media-profile-id | service-id [ service_id ] [ service_id ]...[ service_id ] }
```

Removes a media profile or service id(s).

### Usage

Use this command to configure cnsa media profile ids and service ids. Information for core network authorization is received from HSS. It contains a list of service ids and a media profile id. Since the media profile id is an integer value, the S-CSCF needs to have a static database that contains the mapping between the integer value and the subscribed media profile. The media profile id is assigned to this service policy using the **cnsa-media-profile** command under CSCF Service configuration.

The S-CSCF selects the service profile based on the media profile id set and the policies, such as enforce-codec-policy and video-sessions, will be matched with the incoming request. Other policies, if configured, will be ignored in this scenario.

### Example
The following command defines the media profile id as 2:

```plaintext
cnsa media-profile-id 2
```

The following command defines several service ids:

```plaintext
cnsa service-id xxx:exampletelephony.version1 xxx:abc.com
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
\texttt{end}

Usage
Change the mode back to the Exec mode.
**exit**

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```bash
exit
```

**Usage**

Return to the previous mode.
**filter-criteria**

Configure the filter criteria to be used by this template.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
[ no ] filter-criteria name criteria_name
```

- **no**
  - Removes the specified filter criteria.

- **name criteria_name**
  - Specifies the name of existing filter criteria to be used by this template. The particular criteria applied to a subscriber will be based on the priority parameter. *criteria_name* must be from 1 to 39 alpha and/or numeric characters in length.

**Important:** Filter criteria can be assigned to more than one ISC template.

**Usage**

Use this command to configure the filter criteria to be used by this template.

**Example**

The following command identifies the filter criteria *criteria1*:

```
filter-criteria name criteria1
```
Chapter 59
CSCF Last Route Profile Criteria Configuration Mode Commands

The CSCF Last Route Profile Criteria Configuration Mode is used to configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile. The S-CSCF forwards emergency call packets to the correct Public Safety Answering Point (PSAP) based on this criteria, which it receives from a peer server.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

cscf last-route-profile

name name
criteria { county-name | round-robin}

Last Route Profile Criteria Configuration Mode
```

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

Configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

```
county-name county_name lro-number value
[ no ] county-name county_name
```

- **county_name**
  Specifies the county name.
  *county_name* must be from 1 to 79 alpha and/or numeric characters in length.

- **lro-number value**
  Specifies an existing LRO number.
  *value* can be a maximum of ten digits in length.

- **no county-name county_name**
  Removes the specified county name.

Usage

Use this command to configure county names and assign them LRO numbers.

**Important:** You may configure up to 100 county names.

Example

The following command creates a county name called *norfolk* and assigns it an LRO number of 8884384357:

```
county-name norfolk lro-number 8884384357
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.
**exit**

Exits the current mode and returns to the previous mode.

**Product**

All

**Privilege**

Administrator

**Syntax**

`exit`

**Usage**

Return to the previous mode.
lro-number

Configure the Last Routing Option (LRO) numbers to be used by the CSCF last route profile.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

```
lro-number value

  lro-number value
  Specifies the LRO number.
  value can be a maximum of ten digits in length.

  no
  Removes the specified LRO number.
```

Usage
Use this command to configure LRO numbers.

Important: You may configure up to 100 LRO numbers.

Example
The following command creates an LRO number set at 8884384357:

```
lro-number 8884384357
```
Chapter 60
CSCF Peer Servers Configuration Mode Commands

The CSCF Peer Servers Configuration Mode is used to configure peer servers (for next-hop session routes) within the system.

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

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
**hunting-method**

Configures the method by which servers in this group are contacted.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
hunting-method { round-robin | sequence-on-failure | weighed }
```

```
default hunting-method
```

**round-robin | sequence-on-failure | weighed**

Specifies the hunting method for the servers in this group.

- **round-robin**: Specifies that the servers will be used in round-robin fashion. This is the default setting.
- **sequence-on-failure**: Specifies that the servers will be used sequentially if a failure occurs on a server (i.e., first peer server is always used, except on failure, during which next peer server in the list will be used).
- **weighed**: Specifies that the peer servers in this group have a set “weight” that determines use as compared to the other like-configured peer servers. The actual weight of the peer server is configured in the `server` command in this mode.

**default**

Specifies that the servers will be used in round-robin fashion.

**Usage**

Use this command to configure the method that is used by the system to connect to servers in this group.

**Example**

The following command sets the hunting method for servers in this group to contact sequentially only when a server fails:

```
hunting-method sequence-on-failure
```
server

Configures the name, IP address, and port of servers belonging to this group and enters the Server Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

server name { address ip_address | domain domain_name } [ port number ] [ transport { tcp | udp } ] [ weight number ]

no server name

name
Specifies a name for the server. name must be from 1 to 79 alpha and/or numeric characters in length.

address ip_address
Specifies the IP address of the server. ip_address is expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

domain domain_name
Specifies the domain name of the peer server. domain_name must be from 1 to 255 alpha and/or numeric characters in length.

port number
Specifies the port number of the server. number must be an integer value from 1 to 65535.

transport { tcp | udp }
Specifies the transport type (TCP or UDP).

weight number
Default: 5
Specifies a weighted number for the specific peer server for load balancing purposes. number must be an integer value from 1 to 10. Higher weight implies larger server capability (and more routed requests).

Important: This keyword is only valid if the weighted keyword is applied to the hunting-method command in this mode.

no server name
Removes the specified server from the group.
Usage
Use this command to configure servers belonging to this group and enter the Server Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-server_name-peer-server)#
```

Server Configuration Mode commands are defined in the CSCF Peer Server Monitoring Configuration Mode Commands chapter.

Example
The following command configures a server named `scscf5` with an IP address of `1.2.3.4` and a port number of `5060`:

```
server scscf5 address 1.2.3.4 port 5060
```
Chapter 61
CSCF Peer Server Monitoring Configuration Mode
Commands

The CSCF Peer Server Monitoring Configuration Mode is used to configure an individual peer server’s monitoring parameters and operational mode. It also associates a network session template with the server.
**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```plaintext
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
ims-capable

Indicates whether the peer server belongs to a 3GPP/IMS network or a non-IMS network such as the Internet. This command is used to determine at the S-CSCF whether SIP signaling inter-working is needed when the calls are forwarded to external networks.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
[ no ] ims-capable
```

- **no**
  
  Removes the identification of “IMS capable“ from the selected peer server.

**Usage**

Use this command to identify a peer server as IMS capable allowing the S-CSCF to use SIP signalling inter-working when forwarding calls to non-IMS capable networks.
Iro-selection-profile

Binds a CSCF last route profile with the peer server.

Product
SCM

Privilege
Administrator

Syntax

lro-selection-profile name profile_name

no lro-selection-profile

lro-selection-profile name profile_name
profile_name must be an existing CSCF last route profile and be from 1 to 79 alpha and/or numeric characters.

no lro-selection-profile
Removes CSCF last route profile from the peer server group.

Usage
Use this command to identify a CSCF last route profile to use for finding the correct Public Safety Answering Point (PSAP) during emergency calls.

Example
The following command assigns a CSCF last route profile named lro1 to the peer server group:

lro-selection-profile name lro1

The following command removes a CSCF last route profile from the peer server group:

no lro-selection-profile
mode

Sets the peer server mode to either active or standby. By default, peer servers are in active mode.

Product
SCM

Privilege
Administrator

Syntax

mode { active | standby }

<table>
<thead>
<tr>
<th>active</th>
</tr>
</thead>
</table>
| Defines the mode of the CSCF peer server as active.

<table>
<thead>
<tr>
<th>standby</th>
</tr>
</thead>
</table>
| Defines the mode of the CSCF peer server as standby.

Usage

Use this command to set the peer server mode to either active or standby.

Example
The following command sets the peer server’s mode to standby:

```
mode standby
```
**monitor-status**

Sets parameters for monitoring the status of peer servers.

**Product**

SCM

**Privilege**

Administrator

**Syntax**

```
monitor-status [ monitor-interval seconds ] [ monitor-message options ] [ monitor-response-timer seconds ]
```

**no**

```
no monitor-status
```

**monitor-interval seconds**

Default: 30

Specifies the interval that peer server monitoring will occur. 

- **seconds** must be an integer from 1 to 65535.

**monitor-message options**

Specifies that SIP message (OPTIONS) are to be sent periodically after each monitoring interval.

**monitor-response-timer seconds**

Default: 180

Specifies the interval that the CSCF will wait for responses from the peer server.

- **seconds** must be an integer from 1 to 65535.

**no**

Disables peering server status monitoring.

**Usage**

Use this command to set parameters for monitoring the status of a peer server.

**Example**

The following command sets the monitoring interval to three minutes (180 seconds) and the response timer to six minutes (360 seconds):

```
monitor-status monitor-interval 180 monitor-response-timer 360
```
**nw-session-template**

Specifies a session template for sessions terminating from the peer server group.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
no nw-session-template
```

```
name template-name
```

*template-name* must be an existing session template created in the Session Template Configuration Mode.

**Usage**

Use this command to identify a session template to use for sessions terminating from the peer server group.

**Example**
The following command identifies a session template named *template-25* to use for sessions terminating from the peer server group:

```
nw-session-template template-25
```
Chapter 62
CSCF Policy Configuration Mode Commands

The CSCF Policy Configuration Mode is used to manage AoR policy profiles within the system. User-defined profiles can be managed in this mode.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          csf policy
            { name policy_name }
              Policy Configuration Mode
```

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

Specifies that the newly created policy is an AoR policy and enters the AoR Policy Rules Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

```none
aor-policy-rules
```

Usage
Use this command to create an AoR policy group and enter the AoR Policy Rules Configuration Mode. Entering this command results in the following prompt:
```
[context_name]hostname(config-aor-policy)#
```
AoR Policy Configuration Mode commands are defined in the CSCF AoR Policy Rules Configuration Mode Commands chapter.
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
service-policy-rules

Specifies that the newly created policy is a service policy and enters the Service Policy Rules Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

```
service-policy-rules
```

Usage
Use this command to create a service policy group and enter the CSCF Policy Rules Configuration Mode. Entering this command results in the following prompt:
```
[context_name]hostname(config-service-policy)##
```
Service Policy Rule Configuration Mode commands are defined in the CSCF Policy Rules Configuration Mode Commands chapter.
Chapter 63
CSCF Policy Rules Configuration Mode Commands

The CSCF Policy Rules Configuration Mode is used to manage CSCF AoR and service policy profiles within the system.

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

Configures the policy to allow unauthenticated access. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ default | no ] allow-noauth
```

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>no</td>
</tr>
</tbody>
</table>

Disables the allow-noauth functionality for this policy.

**Usage**

Use this command to allow access to subscribers without authenticating them.
allow-unsecure

Configures the policy to allow access to the system without a security association. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ default | no ] allow-unsecure
```

- `default` | `no`
Disables the allow-unsecure functionality for this policy.

**Usage**
Use this command to enable the policy to provide subscriber access to system without a security association.
authorization

Configures the policy to allow early bandwidth authorization. Default is disabled.

Product
SCM

Privilege
Administrator

Syntax

[ default | no ] authorization early-bandwidth

Usage

Use this command to enable the policy to provide early bandwidth authorization.
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```plaintext
end
```

**Usage**
Change the mode back to the Exec mode.
enforce-codec-policy

Enters the Enforce Codec Policy Command Mode where allowed static and dynamic codec lists are managed.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ default | no ] enforce-codec-policy
```

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
</table>
| Disables the codec policy.

**Usage**

Use this command to enter the Enforce Codec Policy Configuration Mode. Entering this command results in the following prompt:
```
[context_name]hostname(config-policy-enforce-codec)#
```

CSCF Enforce Codec Policy Mode commands are defined in the *Enforce Codec Policy Configuration Mode Commands* chapter in this guide.
**exit**

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
max-cscf-concurrent-sessions

Configures the maximum number of concurrent sessions allowed per subscriber.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
max-cscf-concurrent-sessions number
```

```
default max-cscf-concurrent-sessions
```

*number*  
Default: 5  
Specifies the number of concurrent sessions allowed per subscriber for this policy. *number* must be an integer from 1 to 100.

```
default
```

Resets defaults for this command.

**Usage**

Use this command to set the maximum number of allowed sessions per subscriber for this policy. If enabled, the `subscriber-policy-override` command in the CSCF Service Configuration Mode overrides the service-level policy.

**Example**

The following command sets the maximum number of concurrent sessions for a subscriber using this policy to 7:

```
max-cscf-concurrent-sessions 7
```
policy

Configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to reject subsequent sessions or redirect them to another server.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
policy overload { redirect address1 [ weight weight1 ] [ address2 [ weight weight2 ] ] ... | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }

default policy overload

no policy overload redirect address1[address2] ...
```

*redirect address1 [ weight weight1 ] [ address2 [ weight weight2 ] ] ...

Specifies that upon policy overload, the system will redirect the session to another CSCF.

- `address1`: Must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- `weight weight1`: Defines the priority of the redirect address.
- `weight1`: Must be an integer from 1 to 10. Default is 1.

*reject [ use-reject-code { admin-prohibited | insufficient-resources } ]

Specifies that upon policy overload, the system will reject the session. This is the default setting.

- `use-reject-code`: Specifies that a reject code will be returned upon policy overload.
  - `admin-prohibited`: Specifies that the “admin-prohibited” reject code will be returned upon policy overload.
  - `insufficient-resources`: Specifies that the “insufficient resources” reject code will be returned upon policy overload. This is the default reject code.

*default policy overload

Resets defaults for this command.

*no policy overload redirect address1 [ address2 ] ...

Removes configured policy overload redirect address(es).

Usage

Use this command to define the response to an overload condition on the P-CSCF/A-BG using this AoR policy.

Example
The following command configures the policy overload response to redirect to a series of CSCFs with IP address of 1.2.3.4, 1.2.3.5, and 1.2.3.6 with respective priorities (weights) of 1, 3, and 2:

```
policy overload redirect 1.2.3.4 weight 1 1.2.3.5 weight 3 1.2.3.6 weight 2
```
qos

Configures QoS bandwidth settings for uplink and downlink.

Product
SCM

Privilege
Administrator

Syntax
qos bandwidth { downlink| uplink } [ peak value ]

- **bandwidth { downlink| uplink }
  downlink: Configures the downlink bandwidth.
  uplink: Configures the uplink bandwidth.

- **peak value
  Peak value of bandwidth in kilobits per second (kbit/s).
  value must be an integer from 1 to 99999999.

Usage
The P-CSCF/A-BG fills the required bandwidth for downlink and uplink from the Session Description Protocol (SDP) in the message when communicating with an external policy server via Rx/Tx/Gq. Use this command to configure the peak uplink and downlink bandwidth to be used when the SDP does not contain bandwidth.

Example
Set the peak uplink bandwidth to 256 kbit/s:

qos bandwidth uplink peak 256
video-sessions

Configures the policy to allow video bearers. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ default | no ] video-sessions
```

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
</table>
| Disables the “allow video sessions” feature.

**Usage**

Use this command to allow video session via this policy.
Chapter 64
CSCF Proxy-CSCF Configuration Mode Commands

The Proxy-CSCF Configuration Mode is used to enable Diameter policy control within the service.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

cscf service name

CSCF Service Configuration Mode

proxy-cscf

Proxy-CSCF Configuration Mode
```

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

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

[ no ] allow rfc3261-ua-interworking

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the interworking capability.</td>
</tr>
</tbody>
</table>

Usage
Use this command to enable the P-CSCF/A-BG to allow IMS interworking with RFC3261 SIP User Agents.
diameter

This command:

- configures the Diameter dictionary used in this function.
- configures the policy control origin endpoint used in this function.
- enables the selection of a Diameter policy control peer server providing Rx/Tx/Gq applications for this service.
- configures the Diameter requested timeout value used in this function.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
diameter location-info { dictionary { e2custom01 | e2custom02 | e2custom03 | e2custom04 | e2custom05 | e2custom06 | e2custom07 | e2custom08 | e2custom09 | e2standard } } | origin endpoint endpoint_name | peer-select peer peer_name [ peer-realm realm_name ] | secondary-peer peer_name [ sec-peer-realm realm_name ] | request-timeout sec

diameter policy-control { dictionary { Gq-custom | Gq-standard | Rq-custom | Rx-rel8 | Rx-standard | Tx-standard | custom01 | custom02 | custom03 | custom04 | custom05 | custom06 | custom07 | custom08 | custom09 } } | origin endpoint endpoint_name | peer-select peer peer_name [ peer-realm realm_name ] | secondary-peer peer_name [ sec-peer-realm realm_name ] | request-timeout sec

default diameter { location-info | policy-control } { dictionary | request-timeout }

no diameter { location-info | policy-control } { origin endpoint | peer-select }
```

**location-info**
Defines the E2 interface for location information.

```
dictionary { e2custom01...e2custom09 | e2standard }
```

custom01...custom09: Specifies that a customer-specific (custom) dictionary is to be used for expansion and behaviors.
e2standard: Specifies that the E2-Standard-Dictionary is to be used.

**policy-control**
Defines external policy control.
dictionary { Gq-custom | Gq-standard | Rq-custom | Rx-rel8 | Rx-standard | Tx-standard | custom01...custom09 }

Gq-custom: Specifies that the Gq Operax dictionary is to be used.
Gq-standard: Specifies that the Gq standard dictionary is to be used.
Rq-custom: Specifies that the Rq custom dictionary is to be used.
Rx-rel8: Specifies that the Rx Release 8 dictionary is to be used.
Rx-standard: Specifies that the Rx standard dictionary is to be used.
Tx-standard: Specifies that the Tx standard dictionary is to be used.
custom01...custom09: Specifies that a customer-specific (custom) dictionary is to be used.

origin endpoint endpoint_name
Specifies the Diameter location-info or policy control endpoint name.
endpoint_name must be the endpoint’s name and an alpha and/or numeric string of 1 through 63 characters in length.

peer-select peer peer_name
Specifies the name of the Diameter location-info or policy control peer server.
peer_name must be from 1 to 63 alpha and/or numeric characters in length.
Diameter peer servers are configured through the diameter endpoint command in the Context Configuration Mode. The diameter endpoint command is a generic command and can be found in the Cisco ASR 5000 Series Command Line Interface Reference.

peer-realm realm_name
Specifies the realm name for which the Diameter location-info or policy control peer server has responsibility.
realm_name must be from 1 to 63 alpha and/or numeric characters in length.

**Important:** If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

secondary-peer peer_name
Specifies the name of the secondary Diameter location-info or policy control peer server.
peer_name must be from 1 to 63 alpha and/or numeric characters in length.

sec-peer-realm realm_name
Specifies the realm name for which the secondary Diameter location-info or policy control peer server has responsibility.
realm_name must be from 1 to 63 alpha and/or numeric characters in length.

**Important:** If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

request-timeout sec
Specifies the Diameter location-info or policy control requested timeout value in seconds.
sec must be an integer from 1 to 300.
Default: 10
default diameter { location-info | policy-control } { dictionary | request-timeout }
Sets the Diameter’s location-info or policy control dictionary or requested timeout value as the default.

no diameter { location-info | policy-control } [ origin endpoint | peer-select ]
Removes the Diameter location-info or policy control origin endpoint or Diameter peer from the service.

Usage
Use this command to:
- define the Diameter dictionary to use for the service.
- specify the Diameter origin endpoint.
- specify a Diameter location-info or policy control peer server to support Rx/Tx/Gq applications.
- specify the Diameter requested timeout value for this service.

Example
The following command configures the system to use the Tx standard Diameter dictionary for this service:

    diameter policy-control dictionary Tx-standard

The following command sets the Diameter location-info origin endpoint to test:

    diameter location-info origin endpoint test

The following command selects a Diameter policy control peer server with a name of diam-2 and a realm name of realm-6:

    diameter policy-control peer-select peer diam-2 peer-realm realm-6
emergency-sessions

Configures the function to allow anonymous and/or non-emergency registered subscribers to initiate emergency sessions. The addition of 3GPP IM CN XML body in 380 response messages can also be allowed.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```

[ default | no ] emergency-sessions
```

- **3gpp-ims-xml-body**
  Allow 3GPP IM CN XML body to be added in 380 response messages.

- **anonymous**
  Allow anonymous subscribers to initiate emergency sessions.

- **non-emergency-registered**
  Allow non-emergency registered subscribers to initiate emergency sessions.

- **default**
  Specifies that anonymous and non-emergency registered emergency sessions are allowed and 3GPP IM CN XML body is added in 380 response messages.

- **no**
  Disallows anonymous and/or non-emergency registered emergency sessions and does not add 3GPP IM CN XML body in 380 response messages.

Usage

Use this command to configure the function to allow anonymous and/or non-emergency registered subscribers to initiate emergency sessions. The addition of 3GPP IM CN XML body in 380 response messages can also be allowed.

Example

The following command configures the function to allow only non-emergency registered subscribers to initiate emergency sessions:

```
emergency-sessions non-emergency-registered
```
end

Ends the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax

end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
interrogating-cscf-role

Enables the function to also perform as an Interrogating-CSCF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Syntax**

```
[ no ] interrogating-cscf-role
```

- `no`
  Disables the Interrogating-CSCF role in this function.

**Usage**
Use this command to enable the P-CSCF/A-BG to also perform as an Interrogating-CSCF.

**Important:** All Interrogating-CSCF functions have been moved to the Serving-CSCF exclusively in v10.0 and beyond.
**message-max-size**

Configures the maximum message body size in MESSAGE method.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Syntax**

```
message-max-size limit
[ default | no ] message-max-size
```

*limit*

Default: 1024

Configures the maximum SIP message size limit in bytes for any SIP message buffer. *limit* must be an integer from 512 to 65535.

**Important:** Message body size should be less than the max-sipmsg-size set in the CSCF Service Configuration Mode.

*default | no*

Returns/sets the maximum SIP message size to 1024 bytes.

**Usage**

Use this command to configure the maximum SIP message size for any SIP message buffer.

**Example**

The following command limits the SIP message size to 4000 bytes:

```
message-max-size 4000
```
network-id

Configures the Network Identifier.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

[ no ] network-id id

id
The Network Identifier of the entity.

id must be from 1 to 79 alpha and/or numeric characters in length.

no
Removes the configured Network Identifier of the entity.

Usage
The Network Identifier is used by the P-CSCF or A-BG to fill the P-Visited-Network-ID header.

Example
Sets the Network Identifier to pcscf01.company.com:

    network-id pcscf01.company.com
peer-sbc

Configures peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

[ no ] peer-sbc ip_address

*ip_address*
Specifies the IP address of a peer SBC for this P-CSCF/A-BG service. *ip_address* is expressed in standard dotted decimal notation for IPv4 or colon notation for IPv6.

*no*
Removes the IP address of a peer SBC from this P-CSCF/A-BG service.

Usage
Use this command to specify peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

**Important:** This command must be entered multiple times if more than one SBC is present.

Example
The following commands identify three peer SBCs for a single P-CSCF/A-BG service:

*peer-sbc 200.6.2.3*

*peer-sbc 200.6.2.10*

*peer-sbc 200.6.2.11*

The following command removes the peer SBC with IP address *200.6.2.10* from the P-CSCF/A-BG service:

*no peer-sbc 200.6.2.10*
plmn-id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Syntax**

```
plmn-id mcc code mnc code
no plmn-id
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcc code</td>
<td>Specifies the Mobile Country Code for the mobile access network. <code>code</code> must be a three-digit integer from 200 to 999.</td>
</tr>
<tr>
<td>mnc code</td>
<td>Specifies the Mobile Network Code for the mobile access network. <code>code</code> must be a two or three-digit integer from 00 to 999.</td>
</tr>
<tr>
<td>no plmn-id</td>
<td>Removes the access network configuration for this P-CSCF/A-BG service.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to help match location specific emergency/service numbers when configuring translations. The `mcc` and `mnc` values are compared against those received in `p-access-network-info` headers as per 3GPP TS 24.229. If `mnc` is not provided in the criteria only `mcc` is compared.

**Example**
The following command identifies the mobile network with a MCC of 123 and a MNC of 12:

```
plmn-id mcc 123 mnc 12
```
reg-service-route

Enables the function to use service routes when routing re-registrations.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Syntax**

```
[ no ] reg-service-route
```

```
no

Disables the ability to use service routes for re-registration.
```

**Usage**

Use this command to enable the P-CSCF/A-BG service to use service routes when routing re-registrations.
**reliable-prov-resp**

Enables/disables the reliability of provisional responses feature.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Syntax**

```
reliable-prov-resp { mandatory | optional }
[ no ] reliable-prov-resp
```

- `mandatory`: Both inbound and outbound will request reliability.
- `optional` (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

**no**
Disables the reliability of provisional responses feature.

**Usage**
Use this command to enable/disable the reliability of provisional responses feature.

**Example**
The following command sets the reliability of provisional responses feature to mandatory:

```
reliable-prov-resp mandatory
```

The following command disables the reliability of provisional responses feature:

```
no reliable-prov-resp
```
restoration-procedure

Enables the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or “no response” to service request. This feature is disabled by default.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

[ no ] restoration-procedure

no
Disables restoration procedure on the P-CSCF/A-BG service.

Usage
Restoration procedure is intended to handle unreachability of service-route header content. Enabling this command allows the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or “no response” to service request.

Example
Enables restoration procedure on the P-CSCF/A-BG service:

restoration-procedure

Disables restoration procedure on the P-CSCF/A-BG service:

no restoration-procedure
security-parameters

Enters the Security Configuration Mode in which Denial of Service (DOS) prevention commands can be configured.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
security-parameters
```

Usage
Use this command to enter the Security Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-security-parameters)#
```

Security Configuration Mode commands are defined in the *CSCF Security Configuration Mode Commands* chapter in this guide.
**sigcomp**

Enables signaling compression for the P-CSCF/A-BG service and enters the Signaling Compression Configuration Mode.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Syntax**

```
[ no ] sigcomp
```

- **no**
  
  Disables signaling compression for the P-CSCF/A-BG service.

**Usage**

Use this command to enable signaling compression for the P-CSCF/A-BG service and enter the CSCF Signaling Compression Configuration Mode. Entering this command results in the following prompt:

```
[context_name] hostname(config-sigcomp)#
```

Signaling Compression Configuration Mode commands are defined in the *CSCF Signaling Compression Configuration Mode Commands* chapter in this guide.
## sip-header

Enable SIP P-Access-Network-Info (PANI) or P-User-Database (PUD) header insertion for the P-CSCF/A-BG service.

### Product

SCM (P-CSCF, A-BG)

### Privilege

Administrator

### Syntax

```
[ no ] sip-header insert { p-access-network-info | p-user-database }
```

<table>
<thead>
<tr>
<th><strong>p-access-network-info</strong></th>
<th>Inserts PANI header in received request/response.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>p-user-database</strong></td>
<td>Inserts PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Disables SIP PANI or PUD header insertion for the P-CSCF/A-BG service.</td>
</tr>
</tbody>
</table>

### Usage

Enabling this command allows PANI header insertion in received requests/responses on the P-CSCF or A-BG. In addition, it allows PUD header insertion in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

### Important: Use the access-type command to configure a ue-ip-address-range per access type. CSCF Service Configuration Mode commands are defined in the CSCF Service Configuration Mode Commands chapter in this guide.
**sip-param**

Enable the addition of “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Syntax**

```
[ no ] sip-param insert integrity-protected
```

- **no**
  
  Disables the addition of “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

**Usage**

Enabling this command allows the P-CSCF or A-BG to add the “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message. The parameter will be used by the S-CSCF to decide which authentication mode to use to authenticate the user.

**Example**

Enables the addition of `integrity-protected` parameter:

```
sip-param insert integrity-protected
```

Disables the addition of `integrity-protected` parameter:

```
no sip-param insert integrity-protected
```
store-session-path

Enables the P-CSCF or A-BG to store and process the session path information, which includes the Route list, Record-Route list, Service-Route list, and ViaList.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

[ no ] store-session-path

no

Disables the storing of session path information by the P-CSCF or A-BG. In addition, the P-CSCF/A-BG will not overwrite the Route list, Record-Route list, Service-Route list, or ViaList in the in-dialog request and responses.

Usage
Enabling this command allows the P-CSCF or A-BG to store and process the session path information.

Example
Enables the storage and processing of session path information:

store-session-path

Disables the storage and processing of session path information:

no store-session-path
Chapter 65
CSCF Routes Configuration Mode Commands

The CSCF Routes Configuration Mode is used to configure session forwarding within the system.

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

Places the CSCF route entry at the bottom or end of the route list. Use this command in conjunction with the route command.

Product
SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

Usage
Add this command before the route command to place the entry at the end of the route list.
**before**

Places the CSCF route entry at the top or beginning of the route list. Use this command in conjunction with the `route` command.

**Product**

SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Syntax**

```plaintext
before
```

**Usage**

Add this command before the `route` command to place the entry at the beginning of the route list.
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
end

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
route

Configure the routing parameters for the context.

Product
SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

route { domain name | local { icscf | pcscf | scscf } | nexthop-address address | peer-servers group_name | vpn name } [ [ mod-req-uri ] base-criteria criteria [ filter-criteria1 criteria ] [ filter-criteria2 criteria ] ] [ log ]

no route { domain name | local { icscf | pcscf | scscf } | nexthop-address address | peer-servers group_name | vpn name } base-criteria criteria [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]

domain name
Specifies a valid next-hop domain name. name must be from 1 to 79 alpha and/or numeric characters in length.

local { icscf | pcscf | scscf }
Specifies a local interrogating, serving, or proxy call/session control function to which all calls processed by the context will be routed.

nexthop-address ip_address
Specifies a next-hop address. ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

peer-servers group_name
Specifies a configured peer server group. group_name must be the name of a configured peer server group on this system.

vpn name
Specifies a configured VPN context on the system. name must be a configured context name.

mod-req-uri
Specifies that a route lookup should be performed and the request URI modified.

base-criteria criteria
Specifies the base criteria that packets will be compared against. The following criteria is supported:

• access-type type: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
**3gpp-geran**: 3GPP Access Type
**3gpp-utran-fdd**: 3GPP Access Type
**3gpp-utran-tdd**: 3GPP Access type
**3gpp2-1x**: 3GPP2 Access Type
**3gpp2-1x-hrp**: 3GPP2 Access Type
**3gpp2-umb**: 3GPP2-UMB
**ads1**: FixedLine Access Type
**ads12**: FixedLine Access Type
**ads12p**: FixedLine Access Type ADSL2+
**docsis**: DOCSIS
**gshdsl**: Fixed Line Access Type G.SHDSL
**hdl**: Fixed Line Access Type
**hdsl2**: Fixed Line Access Type
**ids1**: Fixed Line Access Type
**ieee-80211**: WLAN Access Type
**ieee-80211a**: WLAN Access Type
**ieee-80211b**: WLAN Access Type
**ieee-80211g**: WLAN Access Type
**ieee-80216e**: Wireless MAN Access Type
**rads1**: Fixed Line Access Type
**sds1**: Fixed Line Access Type
**vds1**: Fixed Line Access Type
**any**: Filters all CSCF sessions.
**carrier-id name**: Filters sessions based on the carrier’s ID. *name* must be from 1 to 79 alpha and/or numeric characters in length.

**destination aor** *aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

---

**Important**: The destination aor and carried-id criteria cannot occur in the same route rule.

**plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be a two or three-digit integer from 00 to 999.

**source address ip_address**: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**source aor** *aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

**time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for *time-of-day* is as follows:
• **day-of-month** `day`: Filters session based on the day of the month. `day` must be an integer from 1 to 31.

• **day-of-week** `day`: Filters session based on the day of the week. `day` must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.

• **start** `date/time [ end date/time ]`: Filters sessions based on a start time to, optionally, an end time during the day. `date/time` must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. `YYYY`: year range 2005 to 2099, `MM`: months (integer range 1 to 12), `DD`: days (integer range 1 to 31), `HH`: hours (integer range 0 to 23), `mm`: minutes (integer range 0 to 59), `ss`: seconds (integer range 0 to 59).

• **week-of-month** `week`: Filters sessions based on the week of the month. `week` must be an integer from 1 to 5.

---

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

```plaintext
filter-criteria criteria
```

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

• **access-type** `type`: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - `3gpp-geran`: 3GPP Access Type
  - `3gpp-utran-fdd`: 3GPP Access Type
  - `3gpp-utran-tdd`: 3GPP Access Type
  - `3gpp2-1x`: 3GPP2 Access Type
  - `3gpp2-1x-hrpd`: 3GPP2 Access Type
  - `3gpp2-umb`: 3GPP2-UMB
  - `ads1`: Fixed Line Access Type ADSL2+
  - `ads12`: Fixed Line Access Type
  - `ads12p`: Fixed Line Access Type ADSL2+
  - `docsis`: DOCSIS
  - `gshdsl`: Fixed Line Access Type G.SHDSL
  - `hds1`: Fixed Line Access Type
  - `hds12`: Fixed Line Access Type
  - `ids1`: Fixed Line Access Type
  - `ieee-80211`: WLAN Access Type
  - `ieee-80211a`: WLAN Access Type
  - `ieee-80211b`: WLAN Access Type
  - `ieee-80211g`: WLAN Access Type
  - `ieee-80216e`: Wireless MAN Access Type
  - `radsl`: Fixed Line Access Type
**sdsl**: Fixed Line Access Type  
**vdsl**: Fixed Line Access Type  
**any**: Filters all CSCF sessions.  
**carrier-id name**: Filters sessions based on the carrier’s ID. name must be from 1 to 79 alpha and/or numeric characters in length.  
**destination aor aor**: Filters sessions based on the destination AoR. aor must be an existing AoR from 1 to 79 characters in length.

> **Important:** The destination aor and carried-id criteria cannot occur in the same route rule.

**plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. mcc_code must be a three-digit integer from 200 to 999. mnc_code must be a two or three-digit integer from 00 to 999.

**source address ip_address**: Filters sessions based on source IP address. ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**source aor aor**: Filters sessions based on the source AoR. aor must be an existing AoR from 1 to 79 characters in length.

**time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for time-of-day is as follows:

**day-of-month day**: Filters session based on the day of the month. day must be an integer from 1 to 31.

**day-of-week day**: Filters session based on the day of the week. day must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.

**start date/time [ end date/time ]**: Filters sessions based on a start time to, optionally, an end time during the day. date/time must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)

**week-of-month week**: Filters sessions based on the week of the month. week must be an integer from 1 to 5.

> **Important:** AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

**filter-criteria2 criteria**

Specifies the filter criteria that packets that have passed the base criteria and filter-criteria1 will be compared against. The following criteria is supported:

**access-type type**: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:

**3gpp-geran**: 3GPP Access Type  
**3gpp-utran-fdd**: 3GPP Access Type  
**3gpp-utran-tdd**: 3GPP Access type  
**3gpp2-1x**: 3GPP2 Access Type
• **3gpp2-1x-hrp**: 3GPP2 Access Type
• **3gpp2-umb**: 3GPP2-UMB
• **ads1**: FixedLine Access Type
• **ads12**: FixedLine Access Type
• **ads12p**: FixedLine Access Type ADSL2+
• **d sortBy**: DOCSIS
• **gshds1**: Fixed Line Access Type G.SHDSL
• **hds1**: Fixed Line Access Type
• **hds12**: Fixed Line Access Type
• **ids1**: Fixed Line Access Type
• **ieee-80211**: WLAN Access Type
• **ieee-80211a**: WLAN Access Type
• **ieee-80211b**: WLAN Access Type
• **ieee-80211g**: WLAN Access Type
• **ieee-80216e**: Wireless MAN Access Type
• **rads1**: Fixed Line Access Type
• **sds1**: Fixed Line Access Type
• **vds1**: Fixed Line Access Type
• **any**: Filters all CSCF sessions.

**carrier-id name**: Filters sessions based on the carrier’s ID. *name* must be from 1 to 79 alpha and/or numeric characters in length.

**destination aor aor**: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

---

**Important**: The destination aor and carried-id criteria cannot occur in the same route rule.

• **plmn-id mcc mcc code mnc mnc code**: Filters sessions based on the mobile country and network codes. *mcc code* must be a three-digit integer from 200 to 999. *mnc code* must be a two or three-digit integer from 00 to 999.
• **source address ip address**: Filters sessions based on source IP address. *ip address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
• **source aor aor**: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.
• **time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for *time-of-day* is as follows:
  • **day-of-month day**: Filters session based on the day of the month. *day* must be an integer from 1 to 31.
  • **day-of-week day**: Filters session based on the day of the week. *day* must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
**start date/time [ end date/time]:** Filters sessions based on a start time to, optionally, an end time during the day. *date/time* must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)

**week-of-month week:** Filters sessions based on the week of the month. *week* must be an integer from 1 to 5.

---

**Important:** AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

`log`

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility cscf-acl-log` command in the Exec mode.

```plaintext
no route { domain name | local { icscf | pcscf | scscf } | nexthop-address address | peer-servers group_name | vpn name } base-criteria criteria [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]
```

Removes the specified routing parameters for the CSCF service.

---

**Usage**

Use this command to configure routing parameters for the service.

**Important:** Use the `before` or `after` command to place the route entry in the route list.

---

**Example**

The following command is placed at the end of the route list and routes sessions to a peer server group named `icscf_peer5`, filters sessions with a base criteria of the source address (1.2.3.4) and a filter criteria of the destination AoR ($.@test.com):

```plaintext
after route peer-servers icscf_peer5 base-criteria source address 1.2.3.4 filter-criteria1 destination aor $.@test.com
```
Chapter 66
CSCF Service Configuration Mode Commands

The CSCF Service Configuration Mode is used to create and manage CSCF services within the current context.

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

Configures the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses. The access service lets the core service know where a packet needs to be routed.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Syntax**

```plaintext
access-service name name
no access-service [ name name ]
```

- **name name**
  Specifies the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses.
  *name* must be from 1 to 63 alpha and/or numeric characters.

**Important:** This command should only be issued in the core service configuration, however, multiple access services may be configured per core service.

- **no**
  Removes the access service.

**Usage**
Use this command to identify the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses from/to the UEs. This command is used in systems that deploy two P-CSCF/A-BG services in bridging (Back-to-Back User Agent) mode configurations where an access service P-CSCF/A-BG faces the UE network and a core P-CSCF/A-BG faces the public network.

**Example**
The following command identifies the P-CSCF/A-BG access service named to the CSCF/A-BG core service:

```plaintext
access-service name HA3
```
access-type

Specifies the access types for IMS core.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
access-type { 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | 3gpp2-1x | 3gpp2-1x-hrpdp | 3gpp2-umb | adsl | adsl2 | adsl2p | docsis | gshdsl | hds1 | hds12 | idsl | ieee-80211 | ieee-80211a | ieee-80211b | ieee-80211g | ieee-80216e | radsl | sdsl | vdsl } access-profile { default | name access_profile_name } | ue-ip-address-range name ue_ip_name { address ip_address_mask | range start_ip_address end_ip_address }
```

no access-type { 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | 3gpp2-1x | 3gpp2-1x-hrpdp | 3gpp2-umb | adsl | adsl2 | adsl2p | docsis | gshdsl | hds1 | hds12 | idsl | ieee-80211 | ieee-80211a | ieee-80211b | ieee-80211g | ieee-80216e | radsl | sdsl | vdsl } { access-profile | ue-ip-address-range { name ue_ip_name } }

```
access-type { 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | 3gpp2-1x | 3gpp2-1x-hrpdp | 3gpp2-umb | adsl | adsl2 | adsl2p | docsis | gshdsl | hds1 | hds12 | idsl | ieee-80211 | ieee-80211a | ieee-80211b | ieee-80211g | ieee-80216e | radsl | sdsl | vdsl } | 3gpp-geran: 3GPP Access Type 3gpp-utran-fdd: 3GPP Access Type 3gpp-utran-tdd: 3GPP Access Type 3gpp2-1x: 3GPP2 Access Type 3gpp2-1x-hrpdp: 3GPP2 Access Type 3gpp2-umb: 3GPP2-UMB adsl: FixedLine Access Type adsl2: FixedLine Access Type adsl2p: FixedLine Access Type ADSL2+ docsis: DOCSIS gshdsl: FixedLine Access Type G.SHDSL hds1: FixedLine Access Type hds12: FixedLine Access Type idsl: FixedLine Access Type ieee-80211: WLAN Access Type ieee-80211a: WLAN Access Type ieee-80211b: WLAN Access Type ieee-80211g: WLAN Access Type ieee-80216e: Wireless MAN Access Type radsl: FixedLine Access Type sdsl: FixedLine Access Type vdsl: FixedLine Access Type
```

Cisco ASR 5000 Series Command Line Interface Reference
**access-profile** {default | name access_profile_name}

Associates an access type with a CSCF access profile. Different access types can refer to the same access profile.

**ue-ip-address-range** name ue_ip_name { address ip_address_mask | range start_ip_address end_ip_address}

Configures UE IP address/range for a specific access type.

- **ue_ip_name** must be from 1 to 79 alpha and/or numeric characters.
- **address ip_address_mask** Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific access-type applies to. `ip_address_mask` must be specified using the form “IP Address/Mask Bits” where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.
- **range start_ip_address end_ip_address** Configure UE IP range for specific access-type.
  - **start_ip_address** specifies the beginning of the range of addresses.
  - **end_ip_address** specifies the end of the range of addresses.
- **ip_address** must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**no access-type** { 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | 3gpp2-1x | 3gpp2-1x-hrpd | 3gpp2-umb | ads1 | ads12 | ads12p | docsis | gshdsl | hds1 | hds12 | ids1 | ieee-80211 | ieee-80211a | ieee-80211b | ieee-80211g | ieee-80216e | radsl | sds1 | vds1 } [ access-profile | ue-ip-address-range [ name ue_ip_name ] ]

Removes the specified access type from a CSCF access profile or UE IP address/range.

**Usage**

Use this command to associated the access types for a specified CSCF access profile or UE IP address/range name.

**Important:** Use the `sip-header` command to enable SIP P-Access-Network-Info (PANI) header insertion.

CSCF Proxy-CSCF Configuration Mode commands are defined in the *CSCF Proxy-CSCF Configuration Mode Commands* chapter in this guide.

**Example**

The following command identifies the access type adsl and assigns it to access profile `ap1`:

```
access-type adsl access-profile name ap1
```
allow-dereg

Allows the CSCF to send de-registration requests. Feature is disabled by default.

Product
SCM

Privilege
Administrator

Syntax

[ no ] allow-dereg

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the feature.</td>
</tr>
</tbody>
</table>

Usage

Use this command to allow the CSCF service to send de-registration requests. If the UE stops sending keepalive packets, which ends the connection between the UE and the proxy, UE information is cleared from the Proxy-CSCF (P-CSCF) or Access Border Gateway (A-BG). If de-registration requests are enabled, any UE-related information that is shared with the Serving-CSCF (S-CSCF) will also be cleared.
bind

bind

Binds the CSCF service to a logical IP interface and specifies the maximum number of sessions that can access this service over the specified interface.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

bind address ip_address [ access-ipsec-crypto-template template ] [ cscf-hostname host_name ] [ max-sessions max# ] [ port number ] [ reserved-call-capacity percentage] [ transport tcp ] [ use-serviceport-towards-network ]

no bind address

adress ip_address

Specifies the IP address of the interface to which the service is being bound.

ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

access-ipsec-crypto-template template

Specifies the name of an existing IPSec CSCF crypto template to be used for accessing CSCF service by user equipment. Valid only for P-CSCF or A-BG.

template must be an existing IPSec CSCF crypto template and be from 1 to 127 alpha and/or numeric characters.

Important: The IPSec CSCF crypto template should be configured in the same context in which the P-CSCF is configured.

cscf-hostname host_name

Specifies the local host name of the CSCF service.

host_name must be an existing CSCF service name and be from 1 to 127 alpha and/or numeric characters.

Configuring this keyword associates the CSCF service with the AOR domain configured in the default-aor-domain command and uses the domain name in SIP headers.

Important: If this keyword is not configured, SIP headers will contain the IP address of the CSCF service instead of the domain name.

max-sessions max#

Default: 500,000

Specifies the maximum number of sessions managed by this service on this interface.

max# must be configured to any integer value from 0 to 500,000.
Important: The total session capacity of the system is 500,000. `max-sessions` is also limited by the capacity in the license generated for the service. If licenses for PDSN/GGSN/HA are generated for `x` number of sessions, then the license for the CSCF service will be generated at 500,000-`x`. Hardware configuration and installed features can also affect the maximum number of sessions that can be supported.

```
port number
Default: 5060
Specifies the UDP port number.
number must be an integer value from 1 to 65534.
```

```
reserved-call-capacity percentage
Default: 10
Specifies the call capacity percentage per session manager (sessmgr).
percentage must be an integer value from 1 to 50.
```

```
transport tcp
Enables TCP transport for the address.
```

```
use-serviceport-towards-network
Enables use of service port for sending and receiving UDP messages from network elements.
```

```
no bind address
Removes the binding of the service to a specified interface.
```

Usage
Use this command to associated the service with a specific logical IP address. This command also configures the identity of the CSCF in SIP headers as either the domain name of the CSCF service or the IP address.

Important: Multiple keywords can be used per bind command.

Example
The following command binds the CSCF service to a logical interface with an IP address of `1.2.3.4` and sets the maximum number of supported sessions for this interface at `250000`:

```
bind address 1.2.3.4 max-sessions 250000
```
charging

Enables Rf charging in this CSCF service for SIP messages.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ default | no ] charging
```

**default**
Enables Rf charging in this CSCF service for SIP messages.

**no**
Disables Rf charging for this service.

**Usage**

Use this command to enable the RF charging feature in this service and enter the CSCF Charging Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-charging)#
```

CSCF Charging Configuration Mode commands are defined in the *CSCF Charging Configuration Mode Commands* chapter in this guide.
cnsa-media-profile

Configures the media profile id to be set for a previously created service policy.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

[ no ] cnsa-media-profile profile_id cscf-service-policy policy_name content-type { application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml | application-pidf-xml | application-reginfo-xml | application-sdp | application-xml | message-sipfrag | multipart-mixed | multipart-related | text-plain }

no

Removes the media profile from the service policy.

cnsa-media-profile profile_id

Specifies the media profile id.
profile_id must be an integer from 0 to 10 and be an existing media profile id in the system. CNSA media profile ids are created and maintained in the CSCF ISC Template Configuration Mode.

cscf-service-policy policy_name

Assigns the media profile id to a service policy.
policy_name must be from 1 to 63 alpha and/or numeric characters and be an existing policy name in the system. Service policies are created and maintained in the CSCF Policy Configuration Mode.

content-type { application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml | application-pidf-xml | application-reginfo-xml | application-sdp | application-xml | message-sipfrag | multipart-mixed | multipart-related | text-plain }

Specifies the content type(s).
application-3gpp-ims-xml - format for exchanging information in SIP Requests and Responses as used within the 3GPP IM CN Subsystem
application-pidf-diff-xml - contains changed presence elements. Contains full presence document when there are many changes
application-pidf-partial-xml - contains only changed parts of PIDF-based presence information
application-pidf-xml - XML MIME entity that contains presence information
application-reginfo-xml - used in Notifications to SIP user agents about registration expiry
application-sdp - SDP session description
application-xml - content type for generic xml documents
message-sipfrag - contains subsets of well formed SIP messages
multipart-mixed - intended for use when the body parts are independent and need to be bundled in a particular order
multipart-related - intended for compound objects consisting of several inter-related body parts
**Important:** You may specify multiple types of content.

**Usage**
Use this command to assign a media profile id to a service policy. The policies defined in the service policy apply to all subscribers using this service.
CNSA media profile ids are created and maintained in the CSCF ISC Template Configuration Mode. Service policies are created and maintained in the CSCF Policy Configuration Mode.

**Example**
The following command defines the media profile id as 2 and assigns it to `serv_policy3` with plain text content type.

```
cnsa-media-profile 2 cscf-service-policy serv_policy3 content-type text-plain
```
core-service

Configures a core service if:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for Network Address Translation (NAT)

By default, no core-service name will be present.

Product
SCM (CSCF, A-BG)

Privilege
Administrator

Syntax

[ no ] core-service name service_name

no
Removes the core service.

core-service name service_name
Specifies the name of the core service.

service_name must be from 1 to 80 alpha and/or numeric characters.

Usage
Use this command to assign a core service to the CSCF/A-BG service.

Example
The following command identifies the core service:

```
core-service name service1
```
default-aor-domain

Configures the domain name of the service.

Product
SCM

Privilege
Administrator

Syntax

[ no ] default-aor-domain alias

no
Removes the domain name from the service.

default-aor-domain alias
Specifies the domain name for the service.
alias is the name of the domain for this service and must be from 1 to 79 alpha and/or numeric characters in length.

Usage
Use this command to define the domain name of the service.

Example
The following command defines the domain name of the CSCF service as business.com

default-aor-domain business.com
emergency-cscf

Enables the Emergency-CSCF for the service and enters the Emergency-CSCF Configuration Mode. Default is disabled.

Product
SCM

Privilege
Administrator

Syntax

[ no ] emergency-cscf

no
Disables the E-CSCF for the service.

Usage

Use this command to enable the Emergency-CSCF feature and enter the Emergency-CSCF Configuration Mode.

Entering this command results in the following prompt:

[context_name]hostname(config-cscf-service-emergency-cscf)#

Emergency-CSCF Configuration Mode commands are defined in the CSCF Emergency-CSCF Configuration Mode Commands chapter in this guide.

| Important: Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service. |
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

exit

Usage
Return to the previous mode.
history-info

Enables the addition of the history-info header to SIP requests in order to capture request URI information. By default, this command is disabled.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ default | no ] history-info
```

- **default** | **no**
  Disables the inclusion of the history-info header.

**Usage**

Use this command to include the history-info header in SIP requests to capture the request URI information for routing or translation.
interface

Enables interface SIP statistic collection.

Product
SCM

Privilege
Administrator

Syntax

[ no ] interface statistics sip

default | no

Disables interface SIP statistic collection for this service.

Usage

Use this command to enable the collection of interface SIP statistics in this service.
**ipv4-ipv6-interworking**

Allows the P-CSCF to provide IPv4-IPv6 interworking when UEs are IPv6-only and the IMS core network is IPv4-only. Feature is disabled by default.

**Product**  
SCM (P-CSCF)

**Privilege**  
Administrator

**Syntax**

```
[ no ] ipv4-ipv6-interworking
```

- **no**  
  Disables the feature.

**Usage**  
Use this command to allow IPv4-IPv6 interworking functionality.
keepalive

Configures the CSCF to receive and respond to different types of keep-alive requests.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```


no keepalive [ method { crlf | stun } ]
```

### expire-timer sec

Default: 29
This value is used according to timed-keepalives parameter present in Path header. UEs are expected to send keepalive messages according to this time interval.

`sec` must be an integer from 24 to 150.

### max-retry num

Default: 3
Specifies the maximum number of times the CSCF waits for the UE to send a keepalive request before it deletes the user information.

`num` must be an integer from 1 to 10.

### method { crlf | stun }

Default: both methods enabled.
Specifies the method of keepalive messages supported by the CSCF.
- **crlf**: “\r\n” string (CRLF packets) sent by UE
- **stun**: STUN protocol messages (rfc3489-bis)

### Usage

  
  Returns the command to the default settings. All methods are enabled by default. See keywords above for specific defaults.

- **no keepalive [ method { crlf | stun } ]**
  
  Disables the specified method of keepalive messages.
Use this command to configure how the CSCF manages keepalive requests.

Example
The following example sets the expire timer to 40 and the maximum retry parameter to 5:

```
keepalive expire-timer 40 max-retry 5
```
li-packet-cable

Enables the lawful intercept packet cable feature and configures Diameter for Lawful Intercept.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
li-packet-cable diameter { dictionary li-standard | origin endpoint endpoint_name | peer-select peer peer_name [ peer-realm peer_realm ] [ secondary-peer sec_peer_name ] [ sec-peer-realm sec_peer_realm ] }
default li-packet-cable diameter dictionary
no li-packet-cable diameter { origin endpoint | peer-select }
```

**dictionary li-standard**

Configures the li-standard Diameter dictionary.

**origin endpoint endpoint_name**

Specifies the Diameter endpoint. `endpoint_name` must be a string of 1 through 63 characters in length.

**peer-select peer peer_name**

Specifies the Diameter lawful intercept peer. `peer_name` must be a string of 1 through 63 characters in length.

**peer-realm peer_realm**

Specifies the Diameter lawful intercept peer realm. `peer_realm` must be a string of 1 through 63 characters in length.

**secondary-peer sec_peer_name**

Specifies the Diameter lawful intercept secondary peer. `sec_peer_name` must be a string of 1 through 63 characters in length.

**sec-peer-realm sec_peer_realm**

Specifies the Diameter lawful intercept secondary peer realm. `sec_peer_realm` must be a string of 1 through 63 characters in length.

**default li-packet-cable diameter dictionary**

Configures the li-standard Diameter dictionary.
no li-packet-cable diameter { origin endpoint | peer-select }

Disables Diameter Lawful Intercept for the specified function.

Usage
Use this command to enable the lawful intercept packet cable feature and configure Diameter for Lawful Intercept.

Example
The following command defines a Diameter lawful intercept peer named li-peer1:

li-packet-cable diameter peer-select peer li-peer1
max-sipmsg-size

Configures the maximum SIP message size.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

max-sipmsg-size limit

[ default | no ] max-sipmsg-size

*limit*
Default: 4096
Configures the SIP message size limit in bytes.
*limit* must be an integer from 1024 to 65535.

**Important:** Maximum SIP message size should be more than the message-max-size set in the CSCF Proxy-CSCF Configuration Mode.

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
</table>
| Returns/sets the maximum SIP message size to 4096 bytes.

**Usage**
Use this command to configure the maximum SIP message size.

**Example**
The following command limits the SIP message size to *4500* bytes:

```
max-sipmsg-size 4500
```
media-bridging

Enables SDP modification that terminate media on CSCF. Feature is disabled by default.

Product
SCM (P-CSCF)

Privilege
Administrator

Syntax

[ no ] media-bridging

no
Disables the feature.

Usage
Use this command to allow termination of media on CSCF.
nat-policy

Configures a NAT (Network Address Translation) policy for the service if the CSCF service is performing one of the following functions:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

Product
SCM(CSCF, A-BG)

Privilege
Administrator

Syntax

```
nat-policy policy_name { private-address { address ip_address_mask | default | range start_ip_address end_ip_address } | bridge-network { address ip_address_mask | range start_ip_address end_ip_address } }
```

```
no nat-policy policy_name
```

**nat-policy policy_name**

Specifies a name for the NAT policy.  
*policy_name* must be from 1 to 79 alpha and/or numeric characters.

**private-address { address ip_address_mask | default | range start_ip_address end_ip_address }**

Specifies the private-address policy type for nat-pool.  
**address ip_address_mask:** Address for nat-policy policy type for nat-pool. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to.  
*ip_address_mask* must be specified using the form “IP Address/Mask Bits” where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.  
**default:** Default for nat-policy policy type for nat-pool. Default is defined as the address range specified by rfc1918.

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

**range start_ip_address end_ip_address:** Range for nat-policy policy type for nat-pool.  
- **start_ip_address** specifies the beginning of the range of addresses.  
- **end_ip_address** specifies the end of the range of addresses.  
- **ip_address** must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**bridge-network { address ip_address_mask | range start_ip_address end_ip_address }**

Specifies the bridge-network policy type for S-CSCF bridging.
address ip_address_mask: Address for bridge-network policy type for S-CSCF bridging. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to.

ip_address_mask must be specified using the form “IP Address/Mask Bits” here the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.

range start_ip_address end_ip_address: Range for bridge-network policy type for S-CSCF bridging.

• start_ip_address specifies the beginning of the range of addresses.
• end_ip_address specifies the end of the range of addresses.
• ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

no nat-policy policy_name

Removes the specified NAT policy from the service.

Usage

Generally, if a SIP packet has a VIA address (physical address that identifies where the service is located) different from the Source address, ALG functionality is invoked. Even if the VIA and Source addresses are the same, however, this command allows the ALG functionality to be started. For ALG to start, the VIA address should belong to one of the nat-policy address ranges.

Example

The following command identifies the NAT policy named policy1 with a private-address policy type of 10.10.10.10 255.255.255.0:

```
nat-policy policy1 private-address address 10.10.10.10 255.255.255.0
```

The following command identifies the NAT policy named policy2 with a private-address range policy type of 172.162.23.23 172.162.23.230:

```
nat-policy policy2 private-address address 172.162.23.23 172.162.23.230
```

The following command identifies the NAT policy named policy3 with a default policy type:

```
nat-policy policy3 private-address default
```
nat-pool

Configures a NAT (Network Address Translation) pool for the service if the CSCF service is performing one of the following functions:

- P-CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

By default, no nat-pool name will be present.

Product
SCM(P-CSCF, A-BG)

Privilege
Administrator

Syntax

```plaintext
[ no ] nat-pool name pool_name
```

- **no**
  Removes the NAT pool from the service.

- **nat-pool name pool_name**
  Specifies the name of an existing NAT pool.
  `pool_name` must be from 1 to 32 alpha and/or numeric characters.

**Important:** NAT pools are created in Context Configuration Mode with the `ip pool` command.

Usage
Use this command to assign a NAT pool to the P-CSCF/A-BG service.

Example
The following command identifies the NAT pool:

```plaintext
nat-pool name pool2
```
policy

Enables or disables early media support in P-CSCF and configures the congestion control threshold values that are to be monitored on this CSCF service.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Syntax

```
policy { allow-early-media | threshold congestion-control [ system-cpu-utilization percent ] [ tolerance percent ] }

[ default | no ] policy { allow-early-media | threshold congestion-control tolerance }
```

<table>
<thead>
<tr>
<th>allow-early-media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: Enabled</td>
</tr>
<tr>
<td>Allows early media by doing QoS commit during QoS Authorization in P-CSCF.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>threshold congestion-control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables congestion-control.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>system-cpu-utilization percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 80</td>
</tr>
<tr>
<td>The average percent utilization of a CPU in a PSC/PSC2 running the CSCF service as measured in 10 second intervals. percent can be configured to any integer value from 0 to 100. This value becomes the upper threshold for triggering the CPU-based congestion for CSCF services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>tolerance percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 5</td>
</tr>
<tr>
<td>The percentage under a configured threshold that dictates the point at which the condition is cleared. percent is an integer value from 1 to 25.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to the default settings. See keywords above for specific defaults.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the functionality.</td>
</tr>
</tbody>
</table>

Usage
Use this command to set QoS support during either the initial SDP response or the 200OK response to the INVITE. When this CLI is enabled, QoS commit is done during initial SDP answer. When disabled, QoS commit is done during 200OK INVITE. By default, this command is enabled. In addition, thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the CSCF service (congested or clear). The tolerance parameter establishes the threshold at which the condition is cleared.

**Important:** When congestion is triggered, new CSCF calls are not rejected.

**Example**
The following command sets the upper threshold for CPU utilization for triggering congestion control at 90%.

```
 policy threshold congestion-control system-cpu-utilization 90
```

The following command sets the tolerance to its default value of 5.

```
 default policy threshold congestion-control tolerance
```
policy-name

Assigns a previously created service policy to this service.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
policy-name name
no policy-name
```

- **policy-name name**
  Specifies the name of the service policy being assigned to this service.
  *name* must be from 1 to 79 alpha and/or numeric characters and be an existing policy name in the system.
  Service policies are created and maintained in the CSCF Policy Configuration Mode.

- **no**
  Remove the assigned service policy from this service.

**Usage**
Use this command to assign a service policy to this service. The policies defined in the service policy apply to all subscribers using this service. Service policies are created and maintained in the CSCF Policy Configuration Mode.

**Example**
The following command assigns a service policy named *serv_policy3* to this service:

```
policy-name serv_policy3
```
proxy-cscf

Enables the Proxy-CSCF for the service and enters the Proxy-CSCF Configuration Mode. Default is disabled.

Product
SCM (P-CSCF)

Privilege
Administrator

Syntax

[ no ] proxy-cscf

    no
    Disables the P-CSCF for the service.

Usage
Use this command to enable the Proxy-CSCF feature and enter the Proxy-CSCF Configuration Mode. Entering this command results in the following prompt:

    [context_name]hostname(config-cscf-service-proxy-cscf)#

Proxy-CSCF Configuration Mode commands are defined in the CSCF Proxy-CSCF Configuration Mode Commands chapter in this guide.

Important: The Proxy-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
**recurse-on-redirect-resp**

Enables the 3xx recursion feature. If enabled, the service will send further invites to the contacts specified upon receiving a 3xx redirect response. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ no ] recurse-on-redirect-resp
```

- **no**
  Disables the 3xx recursion feature.

**Usage**
When enabled and on receipt of a 3xx response, the service will collect the SIP URIs present in the Contact header(s) of 3xx and recursively contact each one of them until the call succeeds. The contacts are tried serially. There is a maximum implementation limit of 50 URIs. Each contact, in turn, can send a 3xx response. The service will honor them and append the new contacts. When disabled, the service treats a 3xx response as the final failure response and declares the call attempt “failed”. By default, this feature is disabled.

**Example**
Enable recursion on 3xx:

```
recurse-on-redirect-resp
```

Disable recursion on 3xx:

```
no recurse-on-redirect-resp
```
**reject-on-cnsa-failure**

Enables rejection of messages on Core Network Service Authorization failure. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```plaintext
[ no ] reject-on-cnsa-failure
```

- `no`
  
  Disables the rejection of messages on Core Network Service Authorization failure.

**Usage**

Enables rejection of messages on Core Network Service Authorization failure. By default, this feature is disabled.

In a mobile originating case, S-CSCF checks for the presence of P-Preferred-Service (PPS) header. If the header is present, media profile authentication is successful and if the incoming ICSI (IMS Communication Service Identifier) value also matches with one of the values in the service_id list, then the request will be forwarded after replacing the PPS header with PAS (P-Asserted-Service). If media profile authentication fails, S-CSCF will check reject-on-cnsa-failure. If enabled, then call is rejected with 403 message. If disabled, a default ICSI is selected from the service_id list and will be put into PAS while forwarding the request by the S-CSCF on service authentication failure.

In PPS is not received by the S-CSCF and media profile authentication is successful, an ICSI from the service_id list, if present, is selected and will be added in PAS header. If media profile authentication fails, reject-on-cnsa-failure is checked. If enabled, call is rejected with 403 message. If disabled, PAS header is added if service_id list is present with an ICSI value.

**Example**

Enable rejection of messages on Core Network Service Authorization failure:

```
reject-on-cnsa-failure
```

Disable rejection of messages on Core Network Service Authorization failure:

```
no reject-on-cnsa-failure
```
**release-call-on-media-loss**

Release call on detection of media loss.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Syntax**

```
release-call-on-media-loss media-type audio
no release-call-on-media-loss
```

**Usage**

Use this command to enable the release of SIP calls upon the detection of media loss.

**Example**

Enables the release of SIP calls upon the detection of media loss:

```
release-call-on-media-loss media-type audio
```

Enables the release of SIP calls upon the detection of media loss:

```
no release-call-on-media-loss
```
rfc3261-proxy

Enables RFC3261 proxy (SIP Proxy) for this service and enters the SIP Proxy Configuration Mode. Default is disabled.

**Product**
SCM (SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
[ default | no ] rfc3261-proxy
```

*default | no*

Disables RFC3261 proxy in this service.

**Usage**

Use this command to enable the Sip Proxy feature and enter the SIP Proxy Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-rfc3261-proxy)#
```

SIP Proxy Configuration Mode commands are defined in the **CSCF SIP Proxy Configuration Mode Commands** chapter in this guide.

**Important:** The SIP Proxy is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
serving-cscf

Enables Serving-CSCF for the service and enters the Serving-CSCF Command Mode. Default is disabled.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
[ no ] serving-cscf
```

- **no**
  
  Disables S-CSCF for the service.

**Usage**

Use this command to enable the Serving-CSCF feature and enter the Serving-CSCF Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-serving-cscf)##
```

Serving-CSCF Configuration Mode commands are defined in the *CSCF Serving-CSCF Configuration Mode Commands* chapter in this guide.

**Important**: The Serving-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
serving-cscf-list

Configure a list of Serving CSCFs and their capabilities.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ no ] serving-cscf-list server { address address | domain domain } { capability value | port num { capability value } }

no trusted-domain-entity address
```

- **server { address address | domain domain }**
  Specifies the S-CSCF server.
  - **address**
    IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
  - **domain**
    Domain names must be entered using from 1 to 80 alpha and/or numeric characters.

- **capability value**
  Specifies the capability of the S-CSCF server. **value** is assigned by the Service Provider and may be an integer from 1 to 999999.

- **port num**
  Specifies the port at which service is provided by the S-CSCF server. **num** may be an integer from 1 to 65535.

- **no**
  Removes an entry from this list.

**Usage**

Use this command to configure a list of Serving CSCFs and their capabilities.

**Important:** This command can be entered multiple times to identify multiple Serving CSCFs.

**Example**
The following command adds a S-CSCF with an IP address of 1.2.3.4 and a capability value of 75 to this service’s list:

```
serving-cscf-list server address 1.2.3.4 capability 75
```
session-timer

Configures the session expiry for sessions (Session will expire at the configured value unless refreshed.) and the minimum number of seconds in a session timer (session-expires) value the system will allow.

Product
SCM

Privilege
Administrator

Syntax

```
session-timer { min-se sec [ session-expires sec ] | session-expires sec [ min-se sec ] }
```

default session-timer [ min-se ] [ session-expires ]

no session-timer

```
min-se sec
Default: 90
Specifies the minimum number of seconds the system will allow a session-expires value in a session request. sec must be an integer value between 90 and the value of the session-expires command.
```

```
session-expires sec
Default: 1800 (30 minutes)
Specifies the number of seconds a session is allowed exist before it expires. sec must be an integer value between 90 and 18000.
```

default session-timer [ min-se ] [ session-expires ]

Returns the command to the default settings.

```
no
Disables the session timer.
```

Usage
Use this command to set a session expiry value for all invites generated by the SCM and a minimum value for a session request session timer the system will allow. If a session is requested with a timer of less than this command’s value, the system will reject the request with a “422 Session Interval Too Small” response code.

Example
The following command sets the session expiry for all session generated by the SCM to 60 minutes:

```
session-timer session-expires 3600
```

The following command sets the minimum session lifetime value for the service to 270 seconds:

```
session-timer min-se 270
```
strict-outbound

When enabled, the CSCF rejects registration without outbound parameters from an already registered AoR (the AoR would have included outbound parameters in a previous registration). When disabled, the CSCF allows registration without outbound parameters from the previously registered AoR.

Product
SCM

Privilege
Administrator

Syntax

[ no ] strict-outbound

no
Disables the feature. This is the default behavior.

Usage
Use this command to reject registration from a previously registered AoR if the AoR fails to register with outbound parameters but included them in the previous registration.
**subscriber-policy-override**

Configures the system to allow the subscriber-based policy to override the service-based policy. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
[ default | no ] subscriber-policy-override
```

- **default | no**
  Removes the subscriber policy override from the service.

**Usage**

By default, if a conflict occurs between the subscriber-based policy and the service-based policy, the service policy takes precedence. Use this command to override the default behavior of the system and allow the subscriber-based policy to overrule the service policy.
subscription

Enables the registration event package for the service and configures a system-wide subscription lifetime for all subscribers to the service.

Product
SCM

Privilege
Administrator

Syntax

subscription package reg [ lifetime { default sec | max sec [ default sec ] | min sec [ max sec ] [ default sec ] } ]

[ default | no ] subscription package reg

Usage

Use this command to enable the registration event package for the service and control the amount of time subscriptions are allowed to exist on this service. The system responds to subscriptions in the following manner:

Using default values:
- If a subscription with an expiration value lower than the service’s minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a subscription with an expiration value higher than the service’s maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.

If a subscription is received missing the “Expires” value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

Example
The following command configures the maximum subscription lifetime to 43200 (12 hours):

```
subscription package reg lifetime max 43200
```
tcp-proxy

Enables SIP TCP proxy for the CSCF service.

Product
SCM

Privilege
Administrator

Syntax

tcp-proxy [ port port_number ]

no tcp-proxy

port port_number
Default: 5062
Specifies the port used for SIP TCP proxy connections.
port_number must be an integer from 1 to 65534.

no
Disables SIP TCP proxy for the CSCF service

Usage
Use this command to enable SIP TCP proxy for the CSCF service.

Example
Enables SIP TCP proxy for the CSCF service on port 5062:

tcp-proxy port 5062

Disables SIP TCP proxy for the CSCF service:

no tcp-proxy
threshold

Configures the number of route failures that will trigger an alarm.

Product
SCM

Privilege
Administrator

Syntax

```
threshold route-failures high_thresh [ clear low_thresh ]
default threshold route-failures
```

**route-failures high_thresh**
Default: 5
The high threshold number of route failures that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh can be configured to any integer value between 0 and 60000.

**clear low_thresh**
Default: 5
The low threshold number of route failures that must be met or exceeded within the polling interval to clear an alert or alarm. low_thresh can be configured to any integer value between 0 and 60000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

```
default threshold route-failures
```

Returns the command to the default settings.

**Usage**
Use this command to set an alert or an alarm when the number of route failures exceeds the configured level. Alerts or alarms are triggered for the number of registration reply errors on the following rules:
- Enter condition: Actual number of route failures > High Threshold
- Clear condition: Actual number of route failures £ Low Threshold

**Example**
The following command configures a route failures threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold route-failures 1000 clear 500
```
timeout

Sets timeout values for CSCF and SIP transactions.

Product
SCM

Privilege
Administrator

Syntax

timeout { hss-wait sec | no-answer sec | policy-interface sec | sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | d sec | idle-tcp-connection msec | invite-expiry sec | t1 msec | t2 sec | t4 sec } }

timeout { hss-wait | no-answer | policy-interface | sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | d | idle-tcp-connection msec | invite-expiry | t1 | t2 | t4 } }

hss-wait sec
Default: 5
This timer is used by S-CSCF with HSS interface for timeout.
sec must be an integer from 0 to 2147483646.

no-answer sec
Default: 100
This timer is specially used for No-Answer Call Feature executed by S-CSCF. The timer will be started as soon as 180 Ringing response is received and No-Answer call feature is enabled. The value of this timer should be always less than INVITE Timeout used by DC-SIP.
sec must be an integer from 0 to 2147483646.

policy-interface sec
Default: 5
This timer is used by the P-CSCF/A-BG with Policy interface for timeout.
sec must be an integer from 0 to 2147483646.

sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | d sec | idle-tcp-connection msec | invite-expiry sec | t1 msec | t2 sec | t4 sec }

Sets transaction and expiry timers for SIP.

• **3gpp-d sec**: This timer is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport. sec must be an integer from 0 to 2147483646. Default: 64*T1 (128 seconds, recommended minimum)

• **3gpp-t1 msec**: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable
transport. \texttt{msec} must be an integer from 0 to 4294967294. Default: 2000 ms (2 secs, recommended minimum).

\textbf{\texttt{set}} \texttt{sec}: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport. \texttt{sec} must be an integer from 0 to 2147483646. Default: 16 seconds (recommended minimum).

\textbf{\texttt{set}} \texttt{sec}: This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport. \texttt{sec} must be an integer from 0 to 2147483646. Default: 17 seconds (recommended minimum).

\textbf{\texttt{set}} \texttt{sec}: This timer is used to control the retransmission of 200OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport. \texttt{sec} must be an integer from 0 to 2147483646. Default: 64*T1 (32 seconds, recommended minimum)

\textbf{\texttt{set}} \texttt{msec}: This timer is used for closing idle TCP connections. If there is not activity in the TCP connection for the configuration duration, then the connection will be closed. \texttt{msec} must be an integer from 1000 (recommended minimum) to 4294967294. Default: 42000 milliseconds.

\textbf{\texttt{set}} \texttt{sec}: This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport. \texttt{sec} must be an integer from 0 to 2147483646. Default: 100 seconds (recommended minimum).

\textbf{\texttt{set}} \texttt{msec}: Specifies the time interval (in microseconds) between each retransmission. The interval doubles after each retransmission, for example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. \texttt{msec} must be an integer from 0 to 2147483646. Default: 500 milliseconds (recommended minimum).

\textbf{\texttt{set}} \texttt{sec}: This timer is used to control the period for which the request keeps getting retransmitted. This timer is applicable both for reliable and unreliable transport. \texttt{sec} must be an integer from 0 to 2147483646. The recommended minimum value for this parameter is 4 seconds. Default: 64*T1 (32 seconds)

\textbf{\texttt{set}} \texttt{sec}: This timer is used to control the period for which the final response to non-invite transaction should be buffered so as to send the buffered response for the retransmitted non-invite request within that interval. This timer is applicable only for unreliable transport. \texttt{sec} must be an integer from 0 to 2147483646. Default: 5 seconds (recommended minimum).

\textbf{default}

Returns the command to the default settings.

\textbf{Usage}

Use this command to configure SIP Stack timers and CSCF service specific timers.

\textbf{Example}

The following command sets the SIP d timer to 64 seconds:

```bash
timeout sip d 64
```
transport-switching

Sets the message size that triggers a transport protocol switch.

Product
SCM

Privilege
Administrator

Syntax

transport-switching policy protocol tcp trigger msg-size size

default transport-switching policy protocol tcp trigger msg-size

policy protocol tcp trigger msg-size size

Default: 1300
Specifies the size of the SIP message beyond which transport changes to TCP.
size can be configured to any integer value between 1300 and 65535.

default

Returns the size of the SIP message beyond which transport changes to TCP to 1300 bytes.

Usage
Use this command to configure the size of the SIP message beyond which transport changes to TCP.

Example
Switch to TCP transport protocol when the SIP message size is 4000 bytes or more:

transport-switching policy protocol tcp trigger msg-size 4000
trusted-domain-entity

Adds trusted network nodes (or entities) to a table used by this service to identify those nodes that can be trusted with subscriber information.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

```
trusted-domain-entity address [ foreign-network ]
no trusted-domain-entity address
```

**trusted-domain-entity address**
Specifies the IP address of the network node identified as a trusted entity by this service. `address` must be either an IP address or a domain name. IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6. Domain names must be entered using from 1 to 80 alpha and/or numeric characters.

**foreign-network**
Entity belongs to Foreign Network.

**no**
Removes an entry from this service’s trusted domain table.

Usage
Use this command to identify to the service the network entities that can be trusted with subscriber information by this service.

**Important:** This command can be entered multiple times to identify multiple trusted network entities.

Example
The following command adds a network node with an IP address of 1.2.3.4 to this service’s trusted domain table:

```
trusted-domain-entity 1.2.3.4
```
Chapter 67
CSCF Security Configuration Mode Commands

The CSCF Security Configuration Mode is used to configure Denial of Service (DOS) prevention commands.

```
Exec Mode
   configure
      Global Configuration Mode
         context name
            Context Configuration Mode
               csf service name
                  CSCF Service Configuration Mode
                     proxy-cscf
                        Proxy-CSCF Configuration Mode
                           security-parameters
                              CSCF Security Configuration Mode
```

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

Sets a severity number for authorization failures used in calculating a value for determining when to suspend registration attempts.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
auth-failure-weight weight
```

**Default auth-failure-weight**

```plaintext
weight
Default: 1
Assigns a weight to an authorization failure. Defines the severity of a single authorization failure. `weight` must be an integer from 1 to 5.
```

**Usage**

Use this command to define the severity of an authorization failure. This parameter is used in calculating the current number of authorization failures to compare to the `per-aor-failure-limit` and the `per-ip-failure-limit`. Configuring this command with a lower number causes the system to suspend registration attempts with repeated authorization failures much sooner than when configured with a higher number.

**Example**

The following command assigns a weight of 3 to an authorization failure:

```plaintext
auth-failure-weight 3
```
bad-request-weight

Sets a severity number for bad registration requests used in calculating a value for determining when to suspend registration attempts.

Important: The system will ignore the configuration of this command unless the dos-prevention command has been enabled.

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator

Syntax

```
bad-request-weight weight

default bad-request-weight
```

`weight`
Default: 2
Assigns a weight to a bad registration request. Defines the severity of a single bad request. `weight` must be an integer from 1 to 5.

`default`
Sets /restores the default value assigned to the specified command.

Usage
Use this command to define the severity of bad registration request. This parameter is used in calculating the current number of request failures to compare to the per-aor-failure-limit and the per-ip-failure-limit. Configuring this command with a lower number causes the system to suspend registration attempts with repeated request failures much sooner than when configured with a higher number.

Example
The following command assigns a weight of 3 to a bad registration request:
```
bad-request-weight 3
```
dos-prevention

Enables the denial of service prevention feature.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

[ default | no ] dos-prevention

[ default | no ]
Disables the denial of service prevention feature.

Usage

Use this command to enable the denial of service prevention feature. The default value for this command is disabled. When this command is enabled, the commands in this mode are enabled with default values configured.

Important: This command must be enabled before configuring other commands in this mode.
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**
Return to the previous mode.
forking-contact-limit

Sets a limit on the number of contacts a user ID can register with the system.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Syntax**

```
forking-contact-limit limit
```

```
default forking-contact-limit
```

```
limit
Default: 0
Sets the maximum number of contacts a user ID can register with the system. 0 specifies that unlimited contacts can be registered per user ID.

`limit` must be an integer from 0 to 10.

```
default
Sets /restores the default value assigned to the specified command.
```

**Usage**
Use this command to limit the number of contacts a user ID can register with the system.

**Example**
The following command limits all users to 2 registered contacts on the system:

```
forking-contact-limit 2
```
greylist-duration

Configures the amount of time an AoR or IP address remains on a “grey list” after having crossed the registration authorization limit or the bad registration request limit.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
greylist-duration time

default greylist-duration

time
Default: 10
Defines the time, in minutes, that an AoR or IP address remains on a “grey list”.
`time` must be an integer from 5 to 1,440.

default
Sets /restores the default value assigned to the specified command.
```

**Usage**

Use this command to specify the amount of time AoRs or IP addresses remain on a “grey list” after having crossed the registration authorization limit or the bad registration request limit. Limits are described in the `per-aor-failure-limit` command and the `per-ip-failure-limit` command.

**Example**
The following command sets the duration AoRs or IP addresses remain on a “grey list” to 30 minutes:

```plaintext
greylist-duration 30
```
**per-aor-failure-limit**

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending AoR.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Syntax**

```
per-aor-failure-limit limit
default per-aor-failure-limit
```

*limit*
Default: 200
Defines the threshold for registration failures based on a calculation using weighted multipliers defined in `auth-failure-weight` and `bad-request-weight`.
`limit` must be an integer from 5 to 10,000.

**Usage**
Use this command to set a failure limit for registration attempts from an identified AoR. The following calculation determines when this threshold is reached for a specific AoR:
Current authorization failures ÷ `auth-failure-weight` = current failures per AoR
or
Total bad registration requests ÷ `bad-request-weight` = current failures per AoR.
If `auth-failure-weight = 2` and `bad-request-weight = 1`, and the `per-aor-failure-limit = 100`, then the tolerance for registration authentication failures = 50 per AoR and the tolerance for bad registration requests = 100 per AoR.
When an AoR reaches the failure limit, it is added to a “grey list” for a period of time as defined by the `greylist-duration` command.

**Example**
The following command sets the AoR failure limit to 300:

```
per-aor-failure-limit 300
```
per-ip-failure-limit

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending IP address.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Syntax**

```
per-ip-failure-limit limit
default per-ip-failure-limit
```

<table>
<thead>
<tr>
<th>limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 100</td>
</tr>
<tr>
<td>Defines the threshold for registration failures based on a calculation using weighted multipliers defined in <code>auth-failure-weight</code> and <code>bad-request-weight</code>. <code>limit</code> must be an integer from 5 to 10,000.</td>
</tr>
</tbody>
</table>

**default**
Sets /restores the default value assigned to the specified command.

**Usage**
Use this command to set a failure limit for registration attempts from an identified IP address. The following calculation determines when this threshold is reached for any IP address:

- Current authorization failures ÷ `auth-failure-weight` = current failures per AoR
- Total bad registration requests ÷ `bad-request-weight` = current failures per AoR

If `auth-failure-weight` = 2 and `bad-request-weight` = 1, and the `per-ip-failure-limit` = 200, then the tolerance for registration authentication failures = 100 per each IP address and the tolerance for bad registration requests = 200 per each IP address.

When an IP address reaches the failure limit, it is added to a “grey list” for a period of time as defined by the `greylist-duration` command.

**Example**
The following command sets the IP address registration failure limit to 200:

```
per-ip-failure-limit 200
```
threshold-rate

Configures the rate per second at which the system must receive bad requests before it considers the requests a DoS attack.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold-rate rate
```

```
default threshold-rate
```

**rate**
Default: 1
Specifies the rate per second that the system must receive bad requests to determine that it is under a DoS attack.
`rate` must be an integer from 1 to 1,000.

**default**
Sets /restores the default value assigned to the specified command.

**Usage**
Use this command to specify the threshold rate for bad requests. For example, if a malicious user sends bad requests at a rate of 5 per second and this parameter is set to 10, the system will not consider itself under a DoS attack.

**Example**
The following command sets the threshold rate to 5 bad requests per second:

```
threshold-rate 5
```
Chapter 68
CSCF Serving-CSCF Configuration Mode Commands

The Serving-CSCF Configuration Mode is used to set various commands supporting the role of the CSCF service as a Serving CSCF.

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
3gpp

Enables/disables functionality related to 3GPP Release 8 support. This command is disabled by default.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

[ default | no ] 3gpp Rel8

default | no

Disables 3GPP Release 8 support.

Usage

Use this command to configure the S-CSCF to support 3GPP Release 8 functionality.
**alias-indication**

Enables/disables alias indication functionality, a collaborative information exchange between the S-CSCF and HSS. This command is disabled by default.

**Product**  
SCM (S-CSCF, SIP Proxy)

**Privilege**  
Administrator

**Syntax**

```
[ default | no ] alias-indication
```

- `default`  |  `no`
  
  Disables alias indication functionality between the S-CSCF and HSS.

**Usage**

Use this command to display alias information from the HSS.

If both the HSS and the S-CSCF support this feature, Alias Group IDs will be displayed in the output of the `show subscribers cscf-only full` command.

**Important:** 3GPP Release 8 support must be enabled.
allow

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

[ no ] allow rfc3261-ua-interworking

no
Disables the interworking capability.

Usage
Use this command to enable the S-CSCF to allow IMS interworking with RFC3261 SIP User Agents.
**authentication**

Configures the authentication method used by the S-CSCF service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```plaintext
authentication { aka-v1 value | allow-noauth [ invite | re-register | register ] | allow-noipauth [ invite | re-register | register ] | allow-unsecure | aor-auth | md5 value }
```

```plaintext
no authentication { aka-v1 | allow-noauth [ invite | re-register | register ] | allow-noipauth [ invite | re-register | register ] | allow-unsecure | aor-auth | md5 }
```

**aka-v1 value**
Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service. `value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

**Important:** In order to change a priority level, you must remove the original value and configure a new one.

```plaintext
allow-noauth [ invite | re-register | register ]
```

Specifies that access to the S-CSCF service is allowed if authentication fails.

- `invite`: Specifies that access to the S-CSCF service is allowed if authentication fails on INVITE requests only.
- `re-register`: Specifies that access to the S-CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
- `registration`: Specifies that access to the S-CSCF service is allowed if authentication fails on REGISTER requests only.

```plaintext
allow-noipauth [ invite | re-register | register ]
```

Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails.

- `invite`: Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails on INVITE requests only.
- `re-register`: Specifies that access to the S-CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
- `registration`: Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails on REGISTER requests only.

```plaintext
allow-unsecure
```

Specifies that un-secure access is allowed to the S-CSCF service.
**aor-auth**

Specifies that authentication is based on the AoR when accessing the S-CSCF service.

**md5 value**

Specifies that the MD5 algorithm is used as the authentication type for accessing the S-CSCF service. `value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

**Important**: In order to change a priority level, you must remove the original value and configure a new one.

**Usage**

Use this command to configure the authentication method used by the S-CSCF service.

**Important**: The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send “Unknown” in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

- `no authentication { aka-v1 | allow-noauth [ invite | re-register| register ] | allow-noipauth [ invite | re-register| register ] | allow-unsecure | aor-auth | md5 }

Disables the specified authentication method for the S-CSCF service.

**Example**

The following command configures the authentication method used by the S-CSCF service to MD5 with a preference of 3:

```
authentication md5 3
```
diversion-info

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default, diversion-info is disabled.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax
[ default | no ] diversion-info

Usage
Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.
end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

exit

Usage
Return to the previous mode.
ims-restoration

Enables/disables IMS restoration procedures. This feature is disabled by default.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

[ default | no ] ims-restoration

default | no
Disables IMS restoration procedures on the S-CSCF service.

Usage

Use this command to enable IMS REGISTER and INVITE restoration procedures defined in 3GPP TS 23.820.
interrogating-cscf-role

Enables the function to also perform as an Interrogating-CSCF.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

[ no ] interrogating-cscf-role

no

Disables the Interrogating-CSCF role in this function.

Usage

Use this command to enable the S-CSCF to also perform as an Interrogating-CSCF.
local-call-features

Enables/disables local call features. This command is disabled by default.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

[ default | no ] local-call-features

default | no
Disables local call features for this S-CSCF.

Usage
Use this command to enable local call features.
network-id

Configures the Network Identifier.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

```
  network-id id
  [ no ] network-id
```

  `id`

  The Network Identifier of the entity.
  `id` must be from 1 to 79 alpha and/or numeric characters in length.

  `no network-id`

  Removes the configured Network Identifier of the entity.

Usage

The Network Identifier is used to compare with the P-Visited-Network-ID header received from P-CSCF to decide home or roaming subscriber at S-CSCF service.

Example

Sets the Network Identifier to `pcscf01.company.com`:

```
  network-id pcscf01.company.com
```
policy

Configures the policy for Served User Routing in this S-CSCF service.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
[ default | no ] policy allow p-served-user-routing
```

- **allow p-served-user-routing**
  Enables Served User Routing functionality for this S-CSCF.

- **default | no**
  Disables Served User Routing functionality for this S-CSCF.

**Usage**
Use this command to enable/disable the policy for Served User Routing.

**Example**
The following command enables Served User Routing on this service:

```
policy allow p-served-user-routing
```

The following command disables Served User Routing on this service:

```
no policy allow p-served-user-routing
```
**registration**

Configures a registration lifetime for all subscribers to the service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
registration lifetime { default sec | max sec | min sec }
```

```
default registration lifetime
```

<table>
<thead>
<tr>
<th>max sec</th>
<th>min sec</th>
<th>default sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the maximum amount of time that a registration can exist on the system. sec must be an integer from 60 to 2147483646. Default is 86400. max sec must be &gt; or = to min sec.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specifies the minimum amount of time that a registration can exist on the system. sec must be an integer from 60 to max sec -1. Default is 60. min sec must be &lt; or = to max sec.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specifies the default amount of time that a registration can exist on the system. sec must be an integer from 60 to max sec -1. Default is 3761. default sec must be &lt; or = to max sec and &gt; or = to min sec.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

Use this command to control the amount of time registrations are allowed to exist on this service.

The system responds to registrations in the following manner:

Using default values:

- If a registration with an expiration value lower than the service’s minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a registration with an expiration value higher than the service’s maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
- If a registration is received missing the “Expires” value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

**Example**

The following command configures the maximum registration lifetime to 43200 (12 hours):

```
registration lifetime max 43200
```
**reliable-prov-resp**

Enables/disables the reliability of provisional responses feature.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
reliable-prov-resp { mandatory | optional }
no reliable-prov-resp
```

- **mandatory**: Both inbound and outbound will request reliability.
- **optional** (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

**Usage**
Use this command to enable/disable the reliability of provisional responses feature.

**Example**
The following command sets the reliability of provisional responses feature to mandatory:

```
reliable-prov-resp mandatory
```
sifc

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
[ default | no ] sifc
```

<table>
<thead>
<tr>
<th>Default</th>
<th>no</th>
</tr>
</thead>
</table>

Disables shared iFC functionality for this S-CSCF.

**Usage**

Use this command to configure the S-CSCF to share iFC functionality.
If both the HSS and the S-CSCF support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the S-CSCF. The S-CSCF uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.
If the S-CSCF does not support this feature, the HSS will not download identifiers of shared iFC sets.
sip-header

Enable SIP P-User-Database (PUD) header insertion for the S-CSCF service.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
[ no ] sip-header insert p-user-database
```

- `p-user-database`
  Inserts PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

- `no`
  Disables SIP PUD header insertion for the S-CSCF service.

**Usage**

Enabling this command allows PUD header insertion in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.
**sip-request**

Configures SIP Request-related configuration in this S-CSCF service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
sip-request re-route { max-attempts attempts | response-code code }
default sip-request re-route max-attempts
no sip-request re-route response-code code
```

- **re-route**
  Specify SIP Request re-route related configuration.

- **max-attempts attempts**
  Specifies the maximum number of re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.
  *attempts* must be an integer from 1 to 10.
  Default: 2

- **response-code code**
  Specifies the list of Response codes that will be considered as re-routable responses to a call attempt.
  *code* must be a three-digit integer from 400 to 699.

**Important**: You may configure a maximum of five response code values per S-CSCF service.

```
default sip-request re-route max-attempts
```

Specifies a maximum number of two re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.

```
no sip-request re-route response-code code
```

Disables the specified Response code.

**Usage**
Use this command to configure:
- list of Response codes that will be considered as re-routable responses to a call attempt.
- the maximum number of re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.
Example
The following command configures the maximum number of re-route attempts to 5:

```
sip-request re-route max-attempts 5
```
tas

Configures the S-CSCF to perform Telephony Application Server (TAS) functions.

Product
SCM (S-CSCF)

Privilege
Administrator

Syntax

[ default | no ] tas

  default | no
  Disables the TAS feature for this S-CSCF.

Usage
Use this command to configure the S-CSCF to perform TAS functions.
**tas-service**

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
tas-service name
```

```
no tas-service
```

```name```

Specifies the name of the service configured on the system performing TAS functions. *name* must be from 1 to 63 alpha and/or numeric characters and be an existing service.

```no```

Removes the TAS name from the S-CSCF configuration.

**Usage**

Use this command to identify the name of the service configured on the system performing TAS functions.

**Example**

The following command identifies the TAS service name as *scscf3*:

```
tas-service scscf3
```
Chapter 69
CSCF Session Template Configuration Mode Commands

The CSCF Session Template Configuration Mode is used to classify users and/or domains (AoRs) within the system.

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

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
**exit**

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```bash
exit
```

**Usage**
Return to the previous mode.
inbound-cscf-acl

Configures the ACL to use for inbound sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
inbound-cscf-acl { default | name acl_name }
```

```
no inbound-cscf-acl name acl_name
```

<table>
<thead>
<tr>
<th>default</th>
<th>name acl_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>default: Specifies that the default ACL should be used for inbound sessions using this template.</td>
<td>name acl_name: Specifies an existing ACL to use for inbound sessions using this template. acl_name must be the name of an existing ACL.</td>
</tr>
</tbody>
</table>

```
no inbound-cscf-acl name acl_name
```

Removes the ACL from this template.

**Usage**

Use this command to identify an ACL to use on inbound sessions using this template.

**Example**

The following command sets the inbound ACL for this template to an ACL named acl_in22:

```
inbound-cscf-acl name acl_in22
```
outbound-cscf-acl

Configures the ACL to use for outbound sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```plaintext
outbound-cscf-acl { default | name acl_name }

no outbound-cscf-acl name acl_name
```

| **default | name acl_name** |
|-----------|
| default: Specifies that the default ACL should be used for outbound sessions using this template. |
| name acl_name: Specifies an existing ACL to use for outbound sessions using this template. acl_name must be the name of an existing ACL. |

```plaintext
no outbound-cscf-acl name acl_name
```

Removes the ACL from this template.

**Usage**

Use this command to identify an ACL to use on outbound sessions using this template.

**Example**

The following command sets the outbound ACL for this template to an ACL named acl_out22:

```plaintext
outbound-cscf-acl name acl_out22
```
policy-profile

Configures an AoR policy group to be used for sessions using this template.

Product
SCM

Privilege
Administrator

Syntax

```plaintext
policy-profile { default | name profile_name }

no policy-profile name profile_name
```

<table>
<thead>
<tr>
<th>Syntax Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>```plaintext</td>
</tr>
<tr>
<td>default</td>
</tr>
<tr>
<td>default: Specifies that the default policy group will be used for sessions using this template.</td>
</tr>
<tr>
<td>name profile_name: Specifies an existing policy group. profile_name must be an existing CSCF policy group.</td>
</tr>
<tr>
<td>```</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>```plaintext</td>
</tr>
<tr>
<td>no policy-profile name profile_name</td>
</tr>
<tr>
<td>Removes the policy group from the template.</td>
</tr>
<tr>
<td>```</td>
</tr>
</tbody>
</table>

Usage
Use this command to specify a policy group for the template.

Example
The following command specifies that a policy group called `aor_grpl` will be used for sessions using this template:

```plaintext
policy-profile name aor_grpl
```
route-list

Configures a route group to be used for sessions using this template.

Product
SCM

Privilege
Administrator

Syntax

route-list { default | name group_name }

no route-list name group_name

**default | name group_name**

default: Specifies that the default route group will be used for sessions using this template.
name group_name: Specifies an existing route group. group_name must be an existing peer server group.

**no route-list name group_name**

Removes the route group from this template.

Usage

Use this command to specify a route group for the template.

Example

The following command specifies an accounting server group called route_grp2 that will be used for sessions using this template:

```
route-list name route_grp2
```
translation-list

Configures a translation list to be used for sessions using this template.

Product
SCM

Privilege
Administrator

Syntax

translation-list { default | name list_name }

no translation-list name list_name

default | name list_name

default: Specifies that the default translation list will be used for sessions using this template.
name list_name: Specifies an existing translation list. list_name must be an existing translation list.

Usage
Use this command to specify a translation list for the template.

Example
The following command specifies a translation list called trans_list6:

translation-list name trans_list6
urn-service-list

Configures an URN service list to be used for sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
urn-service-list { default | name list_name }

no urn-service-list name list_name
```

- `default | name list_name`
  - `default`: Specifies that the default URN service list will be used for sessions using this template.
  - `name list_name`: Specifies an existing URN service list name. `list_name` must be from 1 to 79 alpha and/or numeric characters and be an existing URN service list.

- `no urn-service-list name list_name`
  - Removes the service list from this template.

**Usage**
Use this command to specify a URN service list for this template. URN service lists are configured in the URN Service List Configuration Mode.

**Example**
The following command specifies that a URN service list named `urn_list5` will be used for sessions using this template:

```
urn-service-list name urn_list5
```
Chapter 70
CSCF Signalling Compression Configuration Mode Commands

The CSCF Signalling Compression Configuration Mode is used to set memory allocation parameters in support of SIP signalling compression. More information regarding signalling compression refer to the IETF RFC 3320 “Signaling Compression (SigComp)”.

![Diagram of CSCF Signalling Compression Configuration Mode]

- Exec Mode
  - configure
    - Global Configuration Mode
      - context name
        - Context Configuration Mode
          - cscf service name
            - CSCF Service Configuration Mode
              - proxy-cscf
                - Proxy-CSCF Configuration Mode
                  - sigcomp
                    - Signaling Compression Config Mode
              - rfc3261-proxy
                - SIP Proxy Configuration Mode
                  - sigcomp
                    - Signaling Compression Config Mode
**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
compression-mode

Configures the dynamic compression mode to be used while sending a SigComp message. Simple dynamic mode is the default.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
compression-mode { multiple-dynamic | simple-dynamic | static | update-dynamic }
```

```
default compression-mode
```

<table>
<thead>
<tr>
<th>multiple-dynamic</th>
<th>simple-dynamic</th>
<th>static</th>
<th>update-dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: simple-dynamic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>multiple-dynamic: A maximum of four dynamic states will be created per compartment. The dynamic states are updated for each message by deleting the oldest dynamic state and creating the new one. The dynamic states will be updated in FIFO (First In, First Out) order.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>simple-dynamic: Only one dynamic state will be created per compartment. The same state will be used for compression.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>static: No dynamic states will be created. Only static dictionary will be used for compression.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>update-dynamic: Only one dynamic state will be created per compartment, but the dynamic state will be updated for every new message.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
default compression-mode
```

Returns the dynamic compression mode to simple dynamic.

**Usage**
Use this command to configure the dynamic compression mode to be used.

**Example**
The following command sets the compression mode to multiple dynamic:

```
compression-mode multiple-dynamic
```

The following command completely disables the creation of dynamic states for compression:

```
compression-mode static
```
decompression-memory-size

Sets the amount of memory available for decompressing one SigComp message. A portion of the allocated memory is used to buffer the message before it is decompressed. The memory is allocated for each SigComp message and is reclaimed once decompression is completed.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```
set compression-memory-size { 128k | 16k | 32k | 64k | 8k }
```

**Default:**

```
set compression-memory-size
```

```
Default: 8k
```

Specifies the amount of memory (in kilobytes) to allocate for decompressing one SigComp message.

```
de compression-memory-size
```

```
default
```

Returns the command to the default settings.

**Usage**

Use this command to set the memory size used to decompress a single SigComp message.

**Example**

The following command sets the memory size for decompressing SigComp messages to 16k:

```
de compression-memory-size 16k```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
state-memory-size

Sets the memory allocated to a compartment for the creation of state. Compartments are application-specific groupings of messages that relate to a peer endpoint. The system allocates memory per compartment. The memory is reclaimed when the system determines that the compartment is no longer required.

Product
SCM

Privilege
Administrator

Syntax

state-memory-size { 4k | 8k }

default state-memory-size

4k | 8k
Default: 4k
Specifies the amount of memory to allocate to a compartment for the creation of state.

default
Returns the command to the default settings.

Usage
Use this command to specify a memory size allocated to message groupings for the creation of state.

Example
The following command sets the state memory size to 8k:

state-memory-size 8k
Chapter 71
CSCF SIP Proxy Configuration Mode Commands

The SIP Proxy Configuration Mode is used to set various commands supporting the role of the CSCF service as a RFC3261-compliant SIP proxy server.

```
Exec Mode
   configure
      Global Configuration Mode
         context name
            Context Configuration Mode
               csf service name
                  CSCF Service Configuration Mode
                     rfc3261-proxy
                        SIP Proxy Configuration Mode
```

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

Enables/disables alias indication functionality, a collaborative information exchange between the CSCF and HSS. This command is disabled by default.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
[ default | no ] alias-indication
```

- **default**
- **no**

Disables alias indication functionality between the CSCF and HSS.

**Usage**

Use this command to display alias information from the HSS.
If both the HSS and the CSCF support this feature, Alias Group IDs will be displayed in the output of the `show subscribers cscf-only full` command.
as-call

Enabling this command causes request-URIs in INVITE messages to be updated with the result of the translation before being passed to an Application Server. This command is disabled by default.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

[ default | no ] as-call invite-request-uri update

default | no

The translation result is ignored.

Usage
Use this command to update the request-URI in INVITE messages with the result of the translation before passing it to an AS.
authentication

Configures the authentication method used by the CSCF service.

Product
SCM (SIP Proxy)

Privilege
Administrator

Syntax

```
authentication { aka-v1 value | allow-noauth [ invite | re-register| register ] |
  allow-noipauth [ invite | re-register| register ] | allow-unsecure | aor-auth |
  md5 value }
```

```
no authentication { aka-v1 | allow-noauth [ invite | re-register| register ] |
  allow-noipauth [ invite | re-register| register ] | allow-unsecure | aor-auth | md5 }
```

```
aka-v1 value
```

Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service. `value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

```
Important: In order to change a priority level, you must remove the original value and configure a new one.
```

```
allow-noauth [ invite | re-register| register ]
```

Specifies that access to the CSCF service is allowed if authentication fails. `invite`: Specifies that access to the CSCF service is allowed if authentication fails on INVITE requests only. `re-register`: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only. `registration`: Specifies that access to the CSCF service is allowed if authentication fails on REGISTER requests only.

```
allow-noipauth [ invite | re-register| register ]
```

Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails. `invite`: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on INVITE requests only. `re-register`: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only. `registration`: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on REGISTER requests only.

```
allow-unsecure
```

Specifies that un-secure access is allowed to the CSCF service.
CSCF SIP Proxy Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aor-auth</td>
<td>Specifies that authentication is based on the AoR when accessing the CSCF service.</td>
</tr>
<tr>
<td>md5 value</td>
<td>Specifies that the MD5 algorithm is used as the authentication type for accessing the CSCF service. value specifies a preference - the lower the value, the higher the preference. value must be an integer from 1 to 1000.</td>
</tr>
</tbody>
</table>

**Important:** In order to change a priority level, you must remove the original value and configure a new one.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no authentication ( aka-v1</td>
<td>allow-noauth [ invite</td>
</tr>
</tbody>
</table>

Disables the specified authentication method for the CSCF service.

**Usage**

Use this command to configure the authentication method used by the CSCF service.

**Important:** The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send “Unknown” in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication allow-noipauth</td>
<td></td>
</tr>
<tr>
<td>allow rfc3261-ua-interworking</td>
<td></td>
</tr>
<tr>
<td>no authentication aka-v1</td>
<td></td>
</tr>
<tr>
<td>no authentication md5</td>
<td></td>
</tr>
</tbody>
</table>

**Example**
The following command configures the authentication method used by the CSCF service to MD5 with a preference of 3:

```
authentication md5 3
```
diversion-info

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default diversion-info is disabled.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

[ default | no ] diversion-info

default | no
The service will not add a diversion header.

Usage
Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.
emergency-sessions

Configures the function to allow anonymous and/or non-emergency registered subscribers to initiate emergency sessions. The addition of 3GPP IM CN XML body in 380 response messages can also be allowed.

Product
SCM (SIP Proxy)

Privilege
Administrator

Syntax

```

[ default | no ] emergency-sessions
```

- **3gpp-ims-xml-body**
  Allow 3GPP IM CN XML body to be added in 380 response messages.

- **anonymous**
  Allow anonymous subscribers to initiate emergency sessions.

- **non-emergency-registered**
  Allow non-emergency registered subscribers to initiate emergency sessions.

- **default**
  Specifies that anonymous and non-emergency registered emergency sessions are allowed and 3GPP IM CN XML body is added in 380 response messages.

- **no**
  Disallows anonymous and/or non-emergency registered emergency sessions and does not add 3GPP IM CN XML body in 380 response messages.

Usage
Use this command to configure the function to allow anonymous and/or non-emergency registered subscribers to initiate emergency sessions. The addition of 3GPP IM CN XML body in 380 response messages can also be allowed.

Example
The following command configures the function to allow only non-emergency registered subscribers to initiate emergency sessions:

```
emergency-sessions non-emergency-registered
```
end

Exits the current mode and returns to theExec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

```
exit
```

Usage
Return to the previous mode.
ims-restoration

Enables/disables IMS restoration procedures. This feature is disabled by default.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
[ default | no ] ims-restoration
```

- **default | no**
  
  Disables IMS restoration procedures on the CSCF service.

**Usage**

Use this command to enable IMS REGISTER and INVITE restoration procedures defined in 3GPP TS 23.820.
registration

Configures a registration lifetime for all subscribers to the service.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

registration lifetime { default sec | max sec | min sec }

default registration lifetime

{ max sec | min sec | default sec }

default sec: Specifies the default amount of time that a registration can exist on the system. sec must be an integer from 60 to max sec -1. Default is 3761. default sec must be < or = to max sec and > or = to min sec.

max sec: Specifies the maximum amount of time that a registration can exist on the system. sec must be an integer from 60 to 2147483646. Default is 86400. max sec must be > or = to min sec.

min sec: Specifies the minimum amount of time that a registration can exist on the system. sec must be an integer from 60 to max sec -1. Default is 60. min sec must be < or = to max sec.

Usage
Use this command to control the amount of time registrations are allowed to exist on this service. The system responds to registrations in the following manner:
Using default values:
• If a registration with an expiration value lower than the service’s minimum (60) is received, the service will respond with a 423 Interval Too Small message.
• If a registration with an expiration value higher than the service’s maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
• If a registration is received missing the “Expires” value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

Example
The following command configures the maximum registration lifetime to 43200 (12 hours):

registration lifetime max 43200
reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

reliable-prov-resp { mandatory | optional }

no reliable-prov-resp

Usage
Use this command to enable/disable the reliability of provisional responses feature.

Example
The following command sets the reliability of provisional responses feature to mandatory:

reliable-prov-resp mandatory

The following command disables the reliability of provisional responses feature:

no reliable-prov-resp
**sifc**

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Syntax**

```
[ default | no ] sifc
```

- **default** | no
Disables shared iFC functionality for this SIP Proxy.

**Usage**

Use this command to configure the SIP Proxy to share iFC functionality.
If both the HSS and the SIP Proxy support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the SIP Proxy. The SIP Proxy uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.
If the SIP Proxy does not support this feature, the HSS will not download identifiers of shared iFC sets.
sigcomp

Enables signaling compression for the SIP Proxy service and enters the Signaling Compression Configuration Mode.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax
[ no ] sigcomp

no
Disables signaling compression for the CSCF service.

Usage
Use this command to enable signaling compression for the SIP Proxy service and enter the CSCF Signaling Compression Configuration Mode.
Entering this command results in the following prompt:

[context_name]hostname(config-sigcomp)#

Signaling Compression Configuration Mode commands are defined in the CSCF Signaling Compression Configuration Mode Commands chapter in this guide.
tas

Configures the SIP Proxy to perform Telephony Application Server (TAS) functions.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

[ default | no ] tas

  default | no
  Disables the TAS feature for this SIP Proxy.

Usage

Use this command to configure the SIP Proxy to perform TAS functions.
tas-service

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Syntax

tas-service name

[ default | no ] tas-service

name
Specifies the name of the service configured on the system performing TAS functions. *name* must be from 1 to 63 alpha and/or numeric characters and be an existing service.

default | no
Removes the TAS name from the SIP Proxy configuration.

Usage
Use this command to identify the name of the service configured on the system performing TAS functions. The ims-sh-service commands are defined in the Context Configuration Mode Commands chapter in this guide.

Example
The following command identifies the TAS service name as *scsf3*:

```
tas-service scsf3
```
The CSCF Translation Configuration Mode is used to configure session re-addressing within the system.

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

Places the CSCF translation entry at the bottom or end of the translation list. Use this command in conjunction with the `uri-readdress` command.

**Product**

SCM

**Privilege**

Administrator

**Syntax**

```text
after
```

**Usage**

Add this command before the `uri-readdress` command to place the entry at the end of the translation list.
before

Places the CSCF translation entry at the top or beginning of the translation list. Use this command in conjunction with the `uri-readdress` command.

**Product**
SCM

**Privilege**
Administrator

**Syntax**
```
before
```

**Usage**
Add this command before the `uri-readdress` command to place the entry at the beginning of the translation list.
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax

exit

Usage
Return to the previous mode.
uri-readdress

Configures readdress criteria for URI translations.

Product
SCM

Privilege
Administrator

Syntax

uri-readdress type trans_type [ log ] { base-criteria criteria } [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]

no uri-readdress type trans_type { base-criteria criteria } [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]

type trans_type

Specifies that the translation list (trans_type) entry is to be identified as one of the following:

blocking-cid: Identifies the translation list entry type as “call ID blocking”.
cancel-blocking-cid: Identifies the translation list entry type as “cancel call ID blocking”.
cancel-cid: Identifies the translation list entry type as “cancel call ID display”.
cancel-cw: Identifies the translation list entry type as “cancel call-waiting”.
cfbi-off: Identifies the translation list entry type as “call forward busy line off”.
cfbi-on: Identifies the translation list entry type as “call forward busy line on”.
cfna-off: Identifies the translation list entry type as “call forward no answer off”.
cfna-on: Identifies the translation list entry type as “call forward no answer on”.
cfu-off: Identifies the translation list entry type as “call forward unconditional off”.
cfu-on: Identifies the translation list entry type as “call forward unconditional on”.
cid: Identifies the translation list entry type as “call ID display”.
cw-off: Identifies the translation list entry type as “call-waiting off”.
cw-on: Identifies the translation list entry type as “call-waiting on”.
directory-assistance: Identifies the translation list entry type as “directory assistance”.
emergency: Identifies the translation list entry type as “emergency”.
international: Identifies the translation list entry type as “international”.
local: Identifies the translation list entry type as “local”.
long-distance: Identifies the translation list entry type as “long-distance”.
one: Identifies the translation list entry type as “any”.
operator-assistance: Identifies the translation list entry type as “operator assistance”.
premium-service: Identifies the translation list entry type as “premium service”.
service: Identifies the translation list entry type as “special service”.
tollfree: Identifies the translation list entry type as “toll free”.

log

Enables logging for CSCF sessions meeting the readdress criteria for URI translations.

base-criteria criteria

Specifies the base criteria that packets will be compared against. The following criteria is supported:

• any: Filters all CSCF sessions.
**destination aor aor**: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

---

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

**plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).

**source address ip_address**: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**source aor aor**: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

**filter-criteria1 criteria**

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.
- **destination aor aor**: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

---

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

**plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).

**source address ip_address**: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**source aor aor**: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

**filter-criteria2 criteria**

Specifies the filter criteria that packets that have passed the base criteria and filter criteria1 will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.
- **destination aor aor**: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

---

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

**plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).
**source address** `ip_address`: Filters sessions based on source IP address. `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**source aor** `aor`: Filters sessions based on the source AoR. `aor` must be an existing AoR from 1 to 79 characters in length.

```plaintext
no uri-readdress type `trans_type` { base-criteria criteria } [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]
```

Remove the readdress configuration.

### Usage

Use this command to readdress URIs based on specified criteria and enters the URI Readdress Configuration Mode. Readdressing can be used for:

- **Mobility**: When roaming in a visited domain.
- **Service Aliases**: Resolving well-known addresses via SIP-AS.
- **Number Translation**: Adding or deleting prefixes such as +1 to/from PSTN numbers.
- **Voice VPNs**: Using inter-office extensions to dial remote offices.

Entering this command results in the following prompt:

```
[context_name]hostname(config-uri-readdress)#
```

URI readdress commands are defined in the CSCF URI Readdress Configuration Mode Commands chapter of this reference.

### Example

The following command readdresses sessions to a domain named `service.com`, filters sessions with a base criteria of the source address `1.2.3.4` and a filter criteria of the destination AoR `.0.test.com`:

```plaintext
uri-readdress type service base-criteria source address 1.2.3.4 filter-criteria1 destination aor $.0.test.com
```
Chapter 73
CSCF URI Readdress Configuration Mode Commands

The URI Readdress Configuration Mode is used to set URI translations.

```
Exec Mode

configure

Global Configuration Mode

c_context name

Context Configuration Mode

ccsf translation name list_name

Translation Configuration Mode

uri-readdress type base-criteria criteria

URI Readdress Configuration Mode
```

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

Adjusts a target address to route sessions to appropriate locations.

**Product**

SCM

**Privilege**

Administrator, Config-administrator

**Syntax**

```
action { addstring| delete num_chars| modifystring} position num target { destination | source } { aor | domain | user }
```

no action

- **add string | delete num_chars | modify string**
  - **add string**: Adds a specified string to a location indicated by the `position` keyword for the targeted source or destination address component (aor, domain, or user). `string` must be from 1 to 79 alpha and/or numeric characters.
  - **delete num_chars**: Deletes a number of characters starting from a location specified by the `position` keyword for the targeted source or destination address component (aor, domain, or user). `num_chars` must be an integer from 1 to 79.
  - **modify string**: Modifies a specified string in a location starting with the `position` keyword for the targeted source or destination address component (aor, domain, or user). The number of characters in the `string` variable will replace the same number in the address. `string` must be from 1 to 79 alpha and/or numeric characters.

- **position num**
  - Specifies the position in the target string where the action is to occur. `num` must be an integer from 1 to 79.

- **target { destination | source }**
  - Specifies that the action is to occur within the source or destination address.

- **aor | domain | user**
  - **aor**: Specifies that the action is applied to AoRs in the targeted source or destination address.
  - **domain**: Specifies that the action is applied to domains in the targeted source or destination address.
  - **user**: Specifies that the action is applied to users in the targeted source or destination address.

**Usage**

Use this command to manipulate SIP packets matching the criteria in the uri-readdress command.
Example
The following command prepends a “+1” to a destination AoR:

```
adon add 1 position 1 target destination aor
```

The following command removes the first two characters from the destination AoR:

```
action delete 2 position 1 target destination aor
```

The following command replaces characters 2 through 4 with the characters “abc” in the destination AoR:

```
action modify abc position 2 target destination aor
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the previous mode.
Chapter 74
CSCF URN List Configuration Mode Commands

The CSCF URN List Configuration Mode is used to map URNs to URIs for emergency and local call services.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          csf urn-service-list name name
            CSCF URN List Configuration Mode
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
cscf-urn-service-mapping

Adds an entry to the service URN mapping table that maps uniform resource names (URNs) to URIs in order to direct specific service-oriented identifiers to the proper location in a network. The table is used after CSCF translation if the result is a local service.

**Product**
SCM

**Privilege**
Administrator

**Syntax**

```shell
[ no ] cscf-urn-service-mapping urn uri uri
```

- **no**
  Removes an entry from the service URN mapping table.

- **urn**
  Specifies the URN to be routed via a URL to the appropriate destination. `urn` must be from 1 to 79 alpha and/or numeric characters.

- **uri**
  Specifies the URI used to route the URN to the appropriate location. `uri` must be from 1 to 79 alpha and/or numeric characters.

**Usage**

Use this command to add an entry to the service URN mapping table that routes a translated URN to a URI for local services.

**Important:** Service URN mapping tables are limited to 30 URN to URI mapping entries.

**Example**
The following command map URN `business` to URI `corp@123.45.678.9:5020` and adds it to the service URN mapping table:

```shell
cscf-urn-service-mapping urn business uri corp@123.45.678.9:5020
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
Chapter 75
CSS Delivery Sequence Configuration Mode Commands

The CSS Delivery Sequence Configuration Mode is used to configure the order in which traffic is delivered to Content Service Steering (CSS) services and their associated content servers.

**Important:** This is a restricted configuration mode. In StarOS 9.0 and later, this configuration mode is deprecated.

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

This is a restricted command. In StarOS 9.0 and later, this command is deprecated.
exit

This is a restricted command. In StarOS 9.0 and later, this command is deprecated.
redirect service (any)

This is a restricted command. In StarOS 9.0 and later, this command is deprecated.
Chapter 76
CSS Service Configuration Mode Commands

The CSS Service Configuration Mode is used to configure properties for Content Service Steering (CSS) services. A CSS service binds a set of delivery interfaces to a service name and specifies a recovery mechanism.

**Important:** This is a restricted configuration mode. In StarOS 9.0 and later, this configuration mode is deprecated.

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

This is a restricted command. In StarOS 9.0 and later, this command is deprecated.
exit

This is a restricted command. In StarOS 9.0 and later, this command is deprecated.
recovery

This is a restricted command. In StarOS 9.0 and later, this command is deprecated.
server-interface

This is a restricted command. In StarOS 9.0 and later, this command is deprecated.
Chapter 77
DHCP Service Configuration Mode Commands

The Dynamic Host Control Protocol (DHCP) Configuration Mode is used to create and manage DHCP service instances for the current context.
bind

This command binds the DHCP service to a logical IP interface facilitating the system’s connection to the DHCP server. This command also configures traffic from the specified DHCP service bind address to use the specified Multiple Protocol Label Switching (MPLS) labels.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

bind address ip_address [ nexthop-forwarding-address nexthop_ip_address [ mpls-label input in_mpls_label_value output out_mpls_label_value1 [ out_mpls_label_value2 ]]]

no bind address ip_address

no

Removes a previously configured binding.

ip_address

Specifies the IP address of an interface in the current context through which the communication with the DHCP server occurs. ip_address must be expressed in dotted decimal notation.

nexthop-forwarding-address nexthop_ip_address

Specifies the next hop gateway address for in MPLS network to which the packets with MPLS labels will be forwarded. nexthop_ip_address must be expressed in IPv4/IPv6 notation.

mpls-label input in_mpls_label_value

This keyword specifies the MPLS label to identify inbound traffic destined for the configured DHCP service bind address ip_address. in_mpls_label_value is the MPLS label that will identify inbound traffic destined for the configured DHCP service and must be an integer from 16 through 1048575.

Important: This keyword is license-enabled and available with valid MPLS feature license only.

Caution: For DHCP over MPLS feature to work in StarOS 9.0 onward dhcp ip vrf command must be configured in DHCP service. Without dhcp ip vrf command the DHCP service using MPLS labels will not be started and as a part of DHCP over MPLS configuration in StarOS 9.0 onward this keyword is a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.
This keyword adds the MPLS label to the outbound traffic sent from the configured DHCP service bind address `ip_address`. The labels `out_mpls_label_value1` and `out_mpls_label_value2` identify the MPLS labels to be added to packets sent from the specified dhcp service bind address.

`out_mpls_label_value1` is the inner output label and must be an integer from 16 through 1048575.

`out_mpls_label_value2` is the outer output label and must be an integer from 16 through 1048575.

**Important:** This keyword is license-enabled and available with valid MPLS feature license only.

**Usage**

Use this command to associate or tie the DHCP service to a specific logical IP address previously configured in the current context and bound to a port. Once bound, the logical IP address or interface is used in the giaddr field of the DHCP packets.

When this command is executed, the DHCP service is started and begins the process of requesting addresses from the DHCP server and storing them in cache memory for allocation to PDP contexts.

This command can also be used to configure MPLS labels for inbound and outbound traffic through this DHCP address.

Only one interface can be bound to a service.

For DHCP over MPLS feature to work in StarOS 9.0 onward `dhcp ip vrf` command must be configured in DHCP service. Without `dhcp ip vrf` command the DHCP service using MPLS labels will not be started.

**Caution:** As a part of DHCP over MPLS configuration `mpls-label input` keyword in `bind address` command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

**Example**

The following command binds the DHCP service to the interface with an IP address of 192.168.1.210:

```
bind address 192.168.1.210
```
default

Restores DHCP service parameters to their factory default settings.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```plaintext
default { dhcp { deadtime | detect-dead-server { consecutive-failures } | server-selection-algorithm } | lease-duration | max-retransmissions | retransmission-timeout | T1-threshold | T2-threshold }
```

- `dhcp { deadtime | detect-dead-server { consecutive-failures } | server-selection-algorithm }` Restores the following DHCP parameters to their respective default settings:
  - `deadtime`: Default 10 minutes
  - `detect-dead-server { consecutive-failures }`: Default 5
  - `server-selection-algorithm`: Default First-server

- `lease-duration` Restores the lease-duration parameter to its default setting of 86400 seconds.

- `max-retransmissions` Restores the max-retransmissions parameter to its default setting of 5.

- `retransmission-timeout` Restores the retransmission-timeout parameter to its default setting of 3000 milli-seconds.

- `T1-threshold` Restores the T1-threshold parameter to its default setting of 50%.

- `T2-threshold` Restores the T2-threshold parameter to its default setting of 88%.

Usage

After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

Example

The following command restores the dhcp deadtime parameter to its default setting of 10 minutes:
default dhcp deadtime
**dhcp client-identifier**

This command configures behavior relating to inclusion of client identifier DHCP option in DHCP messages.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dhcp client-identifier { msisdn | none }
default dhcp client-identifier
```

- **default**
  Sets the behavior of DHCP client identifier to default; i.e. not to include client identifier option in any DHCP message.

- **msisdn**
  Default: disabled
  Specifies that subscriber’s MSISDN be included in client-identifier option of the relevant DHCP messages.

**Important:** This keyword is GGSN license controlled.

- **none**
  Default: enabled
  Specifies that DHCP client-identifier option would not be included in any DHCP messages. This is the default behavior.

**Usage**

Use this command to configure behavior relating to inclusion or exclusion of DHCP client identifier option from DHCP messages.

**Example**
The following command specifies that DHCP client-identifier option be excluded from DHCP messages:

```
dhcp client-identifier none
```
**dhcp deadtime**

Configures the amount of time that the system waits prior to re-communicating with a DHCP server that was previously marked as down.

**Product**
GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dhcp deadtime max_time
```

- `max_time`  
  Default: 10 minutes  
  Specifies the maximum amount of time to wait before communicating with DHCP server that were previously unreachable.
  `max_time` is measured in minutes and can be configured to any integer value from 1 to 65535.

**Usage**

If the system is unable to communicate with a configured DHCP server, after a pre-configured number of failures the system marks the server as being down.

This command specifies the amount of time that the system waits prior to attempting to communicate with the downed server.

**Important:** If all DHCP servers are down, the system will immediately treat all DHCP servers as active, regardless of the deadtime that is specified.

Refer to the `dhcp detect-dead-server` and `max-retransmissions` commands for additional information on the process the system uses to mark a server as down.

**Example**
The following command configures the system to wait 20 minutes before attempting to re-communicate with a dhcp server that was marked as down:

```
dhcp deadtime 20
```
dhcp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a DHCP server as down.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```
dhcp detect-dead-server consecutive-failures max_number
```

```
consecutive-failures max_number
```

Default: 5

Specifies the number of failures that could occur before marking a DHCP server as down. `max_number` could be configured to any integer value from 1 to 1000.

Usage

This command works in conjunction with the `max-retransmissions` parameter to set a limit to the number of communication failures that can occur with a configured DHCP server. The `max-retransmissions` parameter limits the number of attempts to communicate with a server. Once that limit is reached, the system treats it as a single failure. This parameter limits the number of consecutive failures that can occur before the system marks the server as down and communicate with the server of next highest priority.

If all of the configured servers are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority server again.

If the system receives a message from a DHCP server that was previously marked as down, the system immediately treats it as being active.

Example

The following command configures the system to allow 8 consecutive communication failures with a DHCP server before it marks it as down:

```
dhcp detect-dead-server consecutive-failures 8
```
**dhcp ip vrf**

This command provides the DHCP-over-MPLS support and associates the specific DHCP service with a pre-configured Virtual Routing and Forwarding (VRF) Context instance for virtual routing and forwarding.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
dhcp ip vrf vrf_name
no dhcp ip vrf
```

- **no**

  Removes/disassociates configured IP Virtual Routing and Forwarding (VRF) context instance.

- **vrf_name**

  Specifies the name of a pre-configured VRF context instance to be associated with a DHCP service. `vrf_name` is name of a pre-configured virtual routing and forwarding (VRF) context configured in context configuration mode and associated with the IP Pool used by the DHCP service.

**Usage**

Use this command to enable the DHCP-over-MPLS support and to associate/disassociate a pre-configured VRF context to a DHCP service for this feature.

By default the VRF is NULL, which means that DHCP service is bound with binding address given by `bind address` command only.

VRF is not a critical parameter for the DHCP Service but bind address is a critical parameter for DHCP Service, and while starting DHCP Service, if this command is configured, then the bind address should be present in that VRF, and If this command is not configured, bind address should be present in the context where DHCP Service is configured.

For DHCP over MPLS feature to work in StarOS 9.0 onward this command must be configured in DHCP service. Without this command the DHCP service using MPLS labels will not be started.

⚠️ **Caution:** As a part of this configuration `mpls-label input` keyword in `bind address` command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

**Example**

Following command associates VRF context instance `dhcp_vrf1` with this DHCP service:

```
dhcp ip vrf dhcp_vrf1
```
**dhcp server**

Configures DHCP servers with which the DHCP service is to communicate.

**Product**
GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dhcp server ip_address [ priority priority ]
no dhcp server ip_address
```

**no**
Deletes a previously configured DHCP server.

**ip_address**
Specifies the IP address of the DHCP server expressed in dotted decimal notation.

**priority priority**
Specifies the priority of the server if multiple servers are configured. 
`priority` can be configured to any integer value from 1 to 1000. 1 is the highest priority.

**Usage**
Use this command to configure the DHCP server(s) that the system is to communicate with. Multiple servers can be configured each with their own priority. Up to 20 DHCP servers can be configured. All DHCP messages are sent/received on UDP port 67.

**Important:** If a server is removed, all calls having an IP address allocated from the server will be released.

**Example**
The following command configures a DHCP server with an IP address of 192.168.1.200 and a priority of 1:

```
dhcp server 192.168.1.200 priority 1
```
**dhcp server selection-algorithm**

Specifies the algorithm used to select DHCP servers with which to communicate when multiple servers are configured.

**Product**

GGSN, ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
dhcp server selection-algorithm { first-server | round-robin }
```

**first-server**

Default: Enabled

Selects the first-server algorithm to be used. This algorithm dictates that the system select the DHCP servers according to their priority starting with the highest priority server. The system communicates with the server of the next highest priority only when the previous server is unreachable.

**round-robin**

Default: Disabled

Selects the round-robin algorithm to be used. This algorithm dictates that the system communicates with the servers in a circular queue according to the server’s configured priority starting with the highest priority server. The next request is communicated with the next highest priority server, and so on until all of the servers have been used. At this point, the system starts from the highest priority server.

**Usage**

Use this command to determine how configured DHCP servers are utilized by the system.

**Example**

The following command configures the DHCP service to use the round-robin selection algorithm:

```
dhcp server selection-algorithm round-robin
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the context configuration mode and returns to the global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```exit```

**Usage**

Return to the global configuration mode.
lease-duration

Configures the minimum and maximum allowable lease times that are accepted in responses from DHCP servers.

**Product**
GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
lease-duration min min_time max max_time
```

- **min min_time**
  Default: 600
  Specifies the minimum acceptable lease time.
  `min_time` is measured in seconds and can be configured to any integer value from 600 to 3600.

- **max max_time**
  Default: 86400
  Specifies the maximum acceptable lease time.
  `max_time` is measured in seconds and can be configured to any integer value from 10800 to 4294967295.

**Usage**
To reduce the call setup time, the system requests IP addresses from the DHCP server in blocks rather than on a call-by-call basis. Each address received has a corresponding lease time, or time that it is valid. The values configured by command represent the minimum and maximum times that the system allows and negotiates for the lease(s).
If the DHCP server responds with values that are out of the range specified by the min and max values, the system accumulates warning statistics. Responses that fall below the minimum value are rejected by the system and the system contacts the DHCP server with the next highest priority. Responses that are greater than the maximum value are accepted.
When half of the lease time has expired, the system automatically requests a lease renewal from the DHCP server. This is configured using the **Ti-threshold** command.

**Example**
The following command configures the minimum allowable lease time for the system to be 1000 and the maximum to be 36000:

```
lease-duration min 1000 max 36000
```
max-retransmissions

Configures the maximum number of times that the system attempts to communicate with unresponsive DHCP server before it is considered a failure.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

max-retransmissions max_number

- max_number
  Default: 5
  Specifies the maximum number of re-attempts the system tries when no response is received from a DHCP server.
  max_number can be configured to any integer value from 1 to 20.

Usage
This command works in conjunction with the dhcp detect-dead-server parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.
When the value specified by this parameter is met, a failure is logged. The dhcp detect-dead-server parameter specifies the number of consecutive failures that could occur before the server is marked as down.
In addition, the retransmission-timeout command controls the amount of time between re-tries.

Example
The following command configures the maximum number of times the system re-attempts communication with a DHCP server that is unresponsive to 5:

max-retransmissions 5
retransmission-timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the DHCP server.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator

Syntax
retransmission-timeout time

time
Default: 10000
Specifies the time that the system waits before retrying to communicate with the DHCP server.
time is measured in milliseconds and can be configured to any integer value from 100 to 20000.

Usage
This command works in conjunction with the max-retransmissions command to establish a limit on the number of times that communication with a DHCP server is attempted before a failure is logged. This parameter specifies the time between retries.

Example
The following command configures a retry timeout of 1000 milliseconds:

retransmission-timeout 1000
T1-threshold

Configures the DHCP T1 timer as a percentage of the allocated IP address lease.

**Product**
GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
T1-threshold percentage
```

- **percentage**
  - Default: 50%
  - The percentage of the allocated IP address lease time at which the DHCP call-line state is changed to “RENEWING”. It can be configured to any integer value from 40 to 66%.

**Usage**

This command is used to identify the time at which a subscriber must renew their DHCP lease as a percentage of the overall lease time. (Refer to the `lease-duration` command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 40%, then the subscriber would enter the RENEWING state after 4800 seconds.

**Example**

The following command configures the T1 threshold to 40%:

```
T1-threshold 40
```
T2-threshold

Configures the DHCP T2 timer as a percentage of the allocated IP address lease.

**Product**
GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
T2-threshold percentage
```

*percentage*

Default: 88%

The percentage of the allocated IP address lease time at which the DHCP call-line state is changed to “REBINDING”. It can be configured to any integer value from 67 to 99%.

**Usage**

This command is used to identify the time at which a subscriber re-binds their DHCP leased IP address as a percentage of the overall lease time. (Refer to the `lease-duration` command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 70%, then the subscriber would enter the REBINDING state after 8400 seconds.

**Example**
The following command configures the T1 threshold to 70%:

```
T2-threshold 70
```
Chapter 78
Diameter Endpoint Configuration Mode Commands

Diameter Endpoint Configuration Mode is accessed from the Context Configuration Mode. The base Diameter protocol operation is configured in the Diameter Endpoint Configuration Mode.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          diameter endpoint
            endpoint_name
              Diameter Endpoint Configuration Mode
```

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

This command configures the Capabilities-Exchange-Answer (CEA) message timeout duration for Diameter sessions.

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax**

```
cea-timeout timeout
default cea-timeout
```

**default**

Configures the default CEA timeout setting.
Default: 30 seconds

**timeout**

Specifies the timeout duration, in seconds, to make the system wait for this duration for CEA message.
`ttimeout` must be an integer from 1 through 120.

**Usage**

Use this command to configure the CEA timer, i.e., how long to wait for the Capabilities-Exchange-Answer message.

**Example**

The following command sets the Diameter CEA timeout to 16 seconds:
```
cea-timeout 16
```
**connection retry-timeout**

This command configures the Diameter Connection Retry Timeout parameter.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
connection retry-timeout timeout
```

```
default connection retry-timeout
```

```
default
Configures the default Connection Retry Timeout setting.
Default: 30 seconds
```

```
timeout
Specifies the connection retry timeout duration, in seconds, and must be an integer from 1 through 3600.
```

**Usage**

Use this command to configure the Diameter Connection Retry Timeout parameter.

**Example**

The following command sets the Diameter Connection Retry Timer to 120 seconds:

```
connection retry-timeout 120
```
connection timeout

This command configures the Diameter Connection Timeout parameter.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
connection timeout timeout

default connection timeout
```

### default

Configures the default Diameter Connection Timeout setting.
Default: 30 seconds

```
connection timeout timeout
```

*timeout* specifies the connection timeout duration, in seconds, and must be an integer from 1 through 30.

**Usage**

Use this command to configure the Diameter Connection Timeout parameter.

**Example**

The following command sets Diameter connection timeout to 16 seconds:

```
connection timeout 16
```
device-watchdog-request

This command manages transport failure algorithm and configures the number of Device Watchdog Requests (DWRs) that will be sent before a connection is closed.

Product
All

Privilege
Security Administrator, Administrator

Syntax

device-watchdog-request max-retries retry_count

default device-watchdog-request max-retries

**default**

Configures the default setting.
Default: 1

**retry_count**

Specifies the maximum number of DWRs, and must be an integer from 1 through 10.

Usage

Use this command to configure the number of DWRs to be sent before closing the connection from a Diameter endpoint.

Example

The following command sets the DWRs to 3:

device-watchdog-request max-retries 3
**dpa-timeout**

This command configures the Disconnect-Peer-Answer (DPA) message timeout duration for Diameter session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dpa-timeout timeout
```

```
default dpa-timeout
```

---

**default**

Configures the default DPA message timeout setting.

Default: 30 seconds

---

**timeout**

Specifies the DPA message timeout duration, in seconds, and must be an integer from 1 through 60.

---

**Usage**

Use this command to set the timer for DPA message timeout during Diameter connection session. This makes the system wait for this duration for DPA message.

---

**Example**

The following command sets the Diameter DPA timeout to 16 seconds:

```
dpa-timeout 16
```
end

This command returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

   end

Usage
Use this command to change to the Exec mode.
exit

This command exits the Diameter Endpoint Configuration mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
max-outstanding

This command specifies the maximum number of Diameter messages that any application can send to any one peer, awaiting responses.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
max-outstanding messages

{ default | no } max-outstanding

no
Disables the maximum outstanding messages configuration.

default
Configures the default setting.
Default: 256

messages
Specifies the maximum outstanding peer transmit window size setting, and must be an integer from 1 through 4096.
```

**Usage**

Use this command to set the unanswered Diameter messages that any application may send to any one peer, awaiting responses. An application will not send any more Diameter messages to that peer until it has disposed of at least one of those queued messages. It disposes a message by either receiving a valid response or by discarding the message due to no response.

**Example**

The following command sets the Diameter maximum outstanding messages setting to 1024:

```plaintext
max-outstanding 1024
```
origin address

This command has been deprecated. See the origin host and origin realm commands.
**origin host**

This command sets the origin host for the Diameter endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
origin host host_name address ip_address [ port port_number ] [ accept-incoming-connections ] [ address ip_address_secondary ]
no origin host host_name address ip_address [ port port_number ]
```

- **no**
  Removes the origin host configuration.

- **host_name**
  Specifies the host name to bind the Diameter endpoint. `host_name` must be the local Diameter host name, and must be a string of 1 through 255 characters in length.

- **address ip_address**
  Specifies the IP address to bind the Diameter endpoint. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured. `ip_address` must either be an IPv4 address expressed in dotted decimal notation, or an IPv6 address expressed in colon notation.

- **port port_number**
  Specifies the port number for the Diameter endpoint (on inbound connections). `port_number` must be an integer from 1 through 65535.

- **accept-incoming-connections**
  Specifies to accept inbound connection requests for the specified host.

- **address ip_address_secondary**
  Specifies the secondary bind address for the Diameter endpoint. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured. `ip_address_secondary` must either be an IPv4 address expressed in dotted decimal notation, or an IPv6 address expressed in colon notation.

**Usage**

Use this command to set the bind address for the Diameter endpoint.
Diameter agent on chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

The command `origin host host-name` must be entered exactly once. Alternatively, the `origin host host-name address ip_address [ port port_number ]` command may be entered one or more times. The host names should be unique across all endpoints within the context. The address values or address/port combinations should be unique across all endpoints within the context.

---

**Example**
The following command sets the origin host name to `test` and the IP address to `1.1.1.1`:

```
origin host test address 1.1.1.1
```
origin realm

This command configures the realm to use in conjunction with the origin host.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] origin realm realm_name

no
Remove the origin realm configuration.

realm_name
Specifies the realm to bind the Diameter endpoint. The realm is the Diameter identity. The originator’s realm must be present in all Diameter messages. The origin realm can typically be a company or service name. realm_name must be an alpha and/or numeric string of 1 through 127 characters in length.

Usage
Use this command to set the realm for the Diameter endpoint. Diameter agent on chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

Example
The following command sets the origin realm to companyx.

origin realm companyx
**peer**

This command specifies a peer address for the Diameter endpoint.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
peer peer_name [ realm realm_name ] { address ip_address [ [ port port_number ] [ connect-on-application-access ] [ send-dpr-before-disconnect disconnect-cause ] [ sctp ] ] + [ fqn fqn ] [ [ port port_number ] [ send-dpr-before-disconnect disconnect-cause disconnect-cause ] ] }

no peer peer_name [ realm realm_name ]
```

**no**

Removes the specified peer configuration.

**peer_name**

Specifies the peer’s name.

**realm realm_name**

Specifies the realm of this peer.

**address ip_address**

Specifies the Diameter peer IP address. This address must be the IP address of the device the chassis is communicating with.

**fqn fqn**

Specifies the Diameter peer fully qualified domain name (FQDN).

**port port_number**

Specifies the port number for this Diameter peer.

**connect-on-application-access**

Specifies to activate peer on first application access.
**send-dpr-before-disconnect**
Specifies to send Disconnect-Peer-Request (DPR).

**disconnect-cause**
Specifies to send Disconnect-Peer-Request to the specified peer with the specified disconnect reason. The disconnect cause must be an integer from 0 through 2, for one of the following:
- REBOOTING(0)
- BUSY(1)
- DO_NOT_WANT_TO_TALK_TO_YOU(2)

**sctp**
To use Stream Control Transmission Protocol (SCTP) for this peer.

+ Indicates that more than one of the previous keywords can be entered within a single command.

**Usage**
Use this command to add a peer to the Diameter endpoint.

**Example**
The following command adds the peer named test with IP address 1.1.1.1 using port 126:
peer test address 1.1.1.1 port 126
response-timeout

This command configures the Response Timeout parameter.

Product
All

Privilege
Security Administrator, Administrator

Syntax

response-timeout timeout

default response-timeout

default
Configures the default Response Timeout setting.
Default: 60 seconds

timeout
Specifies the response timeout duration, in seconds, and must be an integer from 1 through 300.

Usage
Use this command to configure the Response Timeout parameter.

Example
The following command sets the response timeout to 100 seconds:
response-timeout 100
route-entry

This command creates an entry in the route table for Diameter peer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

route-entry { [ host host_name ] [ peer peer_id [ weight priority ] ] [ realm realm_name { application credit-control peer peer_id [ weight value ] | peer peer_id [ weight value ] } ] ]

no route-entry { [ host host_name ] [ peer peer_id ] [ realm realm_name { application credit-control peer peer_id | peer peer_id } ] ]

no
Disables the specified route-entry table configuration.

host host_name
Specifies the Diameter server’s host name.
host_name must be an alpha and/or numeric string of 1 through 63 characters in length.

realm realm_name
Specifies the realm name. The realm may typically be a company or service name.
realm_name must be an alpha and/or numeric string of 1 through 127 characters in length.

application credit-control
Specifies the credit control application, i.e. DCCA or RADIUS.

peer peer_id
Specifies the peer ID of Diameter endpoint route.
peer_id must be an alpha and/or numeric string of 1 through 63 characters in length.

weight priority
Default: 10
Specifies the priority for a peer in the route table.
The peer with the highest weight is used. If multiple peers have the highest weight, selection is by round-robin mechanism.
priority must be an integer from 0 through 255.

Usage
Use this command to create a route table for Diameter application.
When a Diameter client starts to establish a session with a realm/application, the system searches the route table for the best match. If an entry has no host specified, then the entry is considered to match the requested value. Similarly, if an entry has no realm or application specified, then the entry is considered to match any such requested value. The best match algorithm is to prefer specific matches for whatever was requested, i.e., either realm/application or host/realm/application. If there are no such matches, then system looks for route table entries that have wildcards.

Example
The following command creates a route entry with the host name dcca_host1 and peer ID dcca_peer with priority weight of 10:
```
route-entry host dcca_host1 peer dcca_peer weight 10
```
route-failure

This command controls how action after failure or recovery after failure is performed for the route table.

**Product**
GGSN, ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
route-failure { deadtime seconds | recovery-threshold percent percentage | result-code result_code | threshold counter }
```

```
default route-failure { deadtime | recovery-threshold | threshold }
```

```
no route-failure result-code result_code
```

```
no
```

Disables the route-failure configuration.

```
default
```

Configures the default setting for the specified parameter.

```
deadtime seconds
```

Specifies the time duration, in seconds, for which system keeps the route FAILED status. When this time expires, the system changes the status to AVAILABLE.

`seconds` must be the deadtime duration, in seconds, and must be an integer from 1 through 86400.

Default: 60 seconds

```
recovery-threshold percent percentage
```

Specifies how to reset the failure counter when provisionally changing the status from FAILED to AVAILABLE.

For example, if a failure counter of 16 caused the status to change to FAILED. After the configured deadtime expires, the status changes to AVAILABLE. If this keyword is configured with 75 percent, the failure counter will be reset to 12, i.e., 75 percent of 16.

`percentage` must be the value in percentage of the counter which caused FAILED, and must be an integer from 1 through 99.

Default: 90 percent

```
result-code result_code
```

Configures which answer messages are to be treated as failures, in addition to requests that time out.

Up to 16 different result codes can be specified.

`result_code` must be an integer from 0 through 4,294,967,295.

Default: N/A
threshold counter

Configures the number of errors that causes the status to become FAILED.

Counter must be an integer from 0 through 4,294,967,295.
The error counter begins at zero, and whenever there is a good response it decrements (but not below zero) or increments (but not above this threshold) whenever there is a good response.
Default: 16

Usage

Use this command to control how failure/recovery is performed for the route table. After a session is established, it is possible for the session to encounter errors or Diameter redirection messages that cause the Diameter protocol to re-use the route table to switch to a different route.
Each Diameter client within the chassis maintains counters relating to the status of each of its connections to different hosts (when the destination is realm/application without a specific host, the host name is kept as “”, i.e., blank).
Moreover, those counters are further divided according to which peer is used to reach each host. Each Diameter client maintains a status of each peer-to-host combination. Under normal good conditions the status will be AVAILABLE, while error conditions might cause the status to be FAILED.
Only combinations that are AVAILABLE will be used. If none are AVAILABLE, then system attempts the secondary peer if failover is configured and system can find an AVAILABLE combination there. If nothing is AVAILABLE, system uses a FAILED combination.

Example

The following command configures the time duration for route failure to 90 seconds:

route-failure deadtime 90
tls

This command enables/disables the Transport Layer Security (TLS) support between a Diameter client and Diameter server node.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
tls { certificate certificate | password password | privatekey private_key }
default tls
```

**default**
Configures the default setting.
Default: Disables the TLS support at Diameter endpoint.

**certificate certificate**
Specifies the certificate for TLS support.
*certificate* must be an encrypted certificate, and must be an alpha and/or numeric string of 700 through 900 characters in length.

**password password**
Specifies the password for TLS support.
*password* must be an encrypted password, and must be an alpha and/or numeric string of 6 through 50 characters in length.

**privatekey private_key**
Specifies the private key for TLS support.
*private_key* must be an encrypted key, and must be an alpha and/or numeric string of 900 through 1500 characters in length.

Usage
Use this command to configure TLS support between a Diameter client and Diameter server node. By default, TLS is disabled.

**Important:** Both the Diameter client and server must be configured with TLS enabled or TLS disabled; otherwise, the Diameter connection will be rejected.

Example
The following commands enable the TLS between a Diameter client and Diameter server node:
Diameter Endpoint Configuration Mode Commands

tls certificate "-----BEGIN CERTIFICATE-----
MIICDCAYECAgEBMA0GCSqGSIb3DQEBAU1 mounted
LCJBMNuNRMkwFwyDVQQLExBxWRnZXRzIERpdm1zaW9uMSUwGwYDVQQDEw9UXN0IENBjAwMTA1MTc5MQwCNwMEQwMzA2MTYxMjNDU5MVJRq5swCQYDVQQGEwJUeZTBEEBcHMK
UIRGTSwgsW5jLzEXMBCGA1UEeCwAekBEaXpc2lvbXJEMBAGAIUEeA7b9jYXwob3N0MIGeA0GCSqG
nSIb3DQBEAQUAAgGNA0CBKqBCFQxBdWMjNOP1PLMW4DJBFL2fFE1Kruor0pKw519
nJ0ZYHNW9JHqy6AfQr99ayRdYM0D26h41f0qjDg040XskBaYOFzapSztQMBT
n97OCZ7aHtK8z0ZGNW/cslu+1oOLomgRJcmmIFgW1 RyUUKP1n0hentUdCLLOILO7Q
nCPqZLQIDAQABMA0GCSqGSIb3DQEBAUAA4GAIumU10oWuyN2xfobHYAs+1RLY
nKmFLoI5+iMcGxWXiskmAm+b0PLRAN43wWNUMs8eXgyb
DCrKLv2xWcvKDP3mp7?nAmiVwutv/eFpYz6j38Mo1fsV4y08A/aUXKt23jyKo2hMu8mywkgXCYF2e+7pEeBr
nshbmk8W5Ng0M18eM
-----END CERTIFICATE-----
" tls privatekey "-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
Info: DES-EDE3-CBC,5772A27BE34B611
n1yJ+xAn4MudcIfXXy7E1YngJ9EohIb8yvccyVLMnE4kv0xela/Bghvk25BjYCK5d9nkK8cJgKsEjbc+0xtJxFSbfUhnwKT3wn+sBoJDCPMKkmJXXDbSTOn1sWviAR
nsN84
lHcUHguYoV5s1RJn53f7t7b1nr6xw+C1z6t950QqM1lnkqwekmotVANmch/nccu3N8ghMoPMppmzEv0fOo2/pK2WohcJykSeN5zBrZCUXo0OBNBZcFUcVjR+KsaAn1ZeI1mU60szqg+AOU/XtFccw8RtG1QZK
QbbXzyfbwGA+65qKAhWyKHEI1546wvK
nus1H7J34uUkzoyyyazG6pIGCYV2u/aY013qdmvDqTvmmVIV
veT5g1b3tD99h7D0
n99SHIVoatoPZt4k4YQSVr1351vTs1ZT3OZto4AUw0kLNFYS2ce7pr0reF0K
jV0
n3tgw9pHdMtjHT1k5XqheXZ7TV+rpd2GwCule6201CGWP7os1f2e13e00Y/0
YnPC144aJ
vyP+zuORu7ZBQaS70AA0wV9S83YzW/c15HFIoOeyd8Cu4T1XK11vngbhsaMfCn7aVz1vMzqfpInClcbx+1A6ctIIaYJTUr4d6C4Rbc9RI1G0
njfDWC6a1I9yAgr1R9Wkgd31yAgGe/HDqVXFW148gdY1Q57rHvIqyxrwDmrfv/X1XnMu65LPiDKEc04MEkT7SRZK2C2AzcUXyZ6gA2Vhdbd3AeY2
1nDfd/BRwe5c5
n7eTicCM220I4hBFXDKKsMs37klhoz65Whg6eU31D0Tzd76xOStg=
-----END RSA PRIVATE KEY-----
" tls password_for_TLS
use-proxy

This command enables/disables Diameter proxy for the Diameter endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] use-proxy
```

- **no**
  Disables Diameter proxy for the current endpoint.
  This command at endpoint level will actually equip an application to use Diameter proxy to route all its messages to external peer.

**Usage**

By default, the use-proxy configuration is disabled.
This command equips an application to use Diameter proxy to route all its messages to external peer. The proxy acts as an application gateway for Diameter. It gets the configuration information at process startup and decides which Diameter peer has to be contacted for each application. It establishes the peer connection upon finding no peer connection already exists.
Each proxy task will automatically select one of the host names configured with the `origin host` CLI command. Multiple proxy tasks will not use the same host names, so there should be at least as many host names as proxy tasks. Otherwise, some proxy tasks will not be able to perform Diameter functionality. The chassis automatically selects which proxy tasks are used by which managers (i.e., ACSMgs/SessMgs), without verifying whether the proxy task is able to perform Diameter functionality.
To be able to run this command, the Diameter proxy must be enabled. In the Global Configuration Mode, see the `require diameter-proxy` CLI command.

**Example**
The following command enables Diameter proxy for the current endpoint:
```
use-proxy
```
The following command disables Diameter proxy for the current endpoint:
```
no use-proxy
```
**watchdog-timeout**

This command configures the Watchdog Timeout parameter.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
watchdog-timeout timeout

{ default | no } watchdog-timeout
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the watchdog timeout configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the default watchdog timeout setting.</td>
</tr>
<tr>
<td>Default: 30 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the timeout duration, in seconds, and must be an integer from 6 through 30.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure the Watchdog Timeout parameter for the Diameter endpoint. If this timer expires before getting a response from the destination, other route to the same destination is tried, as long as the retry count setting has not been exceeded (see the device-watchdog-request CLI command) and as long as the response timer has not expired (see the response-timeout CLI command).

**Example**
The following command sets the watchdog timeout setting to 15 seconds:

```
watchdog-timeout 15
```
Chapter 79
DLCI Configuration Mode Commands

The DLCI configuration mode provides the commands to configure, bind and manage the DLCI associated with a specific port defined in the parent configuration mode, Channelized Port configuration mode.

```
Exec Mode

configure

Global Configuration Mode

port channelized slot/port

Channelized Port Configuration Mode

dlci path path_id {ds1|e1} num_con dlci dlci_id

DLCI Configuration Mode
```

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

This command configures an association (binds) between an IP interface or a pre-configured routing SS7/Frame Relay link and the specific port being configured with the Channelized Port configuration commands.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bind link peer-nsei nse_id ns-vci ns-vc_id
no bind link peer-nsei nse_id ns-vci ns-vc_id
```

- **peer-nsei nse_id**
  Defines the end-point network service entity identifier (NSEI). The NSEI must be an integer from 0 to 65535.

- **ns-vc-id ns-vc_id**
  Defines the network service virtual circuit identifier (NSVCI). The NSVCI must be an integer from 0 to 65535.

- **no**
  Deletes the bind configuration from the Operator Policy.

**Usage**

Bind this port to network service entity 2 and network service VC 234.

**Example**

```
bind link peer-nsei 2 ns-vci 234
```
end

Exits this sub-configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode and return to the Exec mode.
exit

Exits the this sub-configuration mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the previous configuration mode.
shaping

Defines egress traffic shaping to control flow for this DLCI.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

shaping type

default shaping

shaping type
The following types of shaping provide flow management:
- cir: Committed Info Rate
- cir-eir: Committed Info Rate with Excess Rate
- ppr: Peak Packet Rate
- wfq: Weighted Fair Queuing

default
Resets the DLCI configuration to the system default.

Usage
Use this command to identify the type of signal shaping to be used on the DLCI.

Example

shaping cir
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the no keyword enables the port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

`shutdown`

`no shutdown`

```
no

Enables the port’s administrative state. When omitted the card is shutdown (removed from service).
```

Usage

Shut down a port prior to re-cabling and/or other maintenance activities. This command with the no keyword is required to bring a port into service.

Example

```
shutdown
no shutdown
```
The DNS Client Configuration Mode is used to manage the system’s DNS interface and caching parameters.

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

Binds the DNS client to a pre-configured logical IP interface.

**Product**
SCM, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bind address ip_address [ port number ]
no bind address
```

- **no**
  Removes the binding of the client to a specified interface.

- **ip_address**
  Specifies the IP address of the interface to which the DNS client is being bound. `ip_address` must be expressed in IPv4 dotted decimal notation.

- **port number**
  Default: 6011
  Specifies the UDP port number of the interface to which the DNS client is being bound. `number` must be an integer value from 1 to 65535.

**Usage**
Use this command to associate the client with a specific logical IP address.

**Example**
The following command binds the DNS client to a logical interface with an IP address of 1.2.3.4 and a port number of 6000:

```
bind address 1.2.3.4 port 6000
```
cache algorithm

Configures the method of use of the DNS VPN and session cache.

**Product**
SCM, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cache algorithm { central | local } { FIFO | LRU | LFU }
default cache algorithm { central | local }
```

- **default**
  Sets the DNS VPN and session cache method to default setting.

- **central | local**
  central: Specifies the central proclet (VPN manager)
  local: Specifies the local proclet (session manager)

- **FIFO | LRU | LFU**
  FIFO: First in first out. This is the default setting for the central proclet.
  LRU: Least recently used. This is the default value for the local proclet.
  LFU: Least frequently used.

**Usage**

Use this command to configure the method by which entries are added and removed from the DNS cache.

**Example**

The following command configures the cache algorithm for the central proclet to least frequently used (LFU):

```
cache algorithm central lfu
```
cache size

Configures the maximum number of entries allowed in the DNS cache.

Product
SCM, SGSN

Privilege
Security Administrator, Administrator

Syntax

cache size { central | local } max_size

default cache size { central | local }

default
Sets the maximum number of entries allowed in the DNS cache to default setting.

{ central | local } max_size

central max_size: Specifies the maximum number of entries allowed in the central proclet cache. max_size must be an integer value from 100 to 65535 in length. The default value for the central proclet is 50000.

local max_size: Specifies the maximum number of entries allowed in the local proclet cache. max_size must be an integer value from 100 to 65535 in length. The default value for the local proclet is 1000.

Usage
Use this command to configure the maximum number of entries allowed in the DNS cache.

Example
The following command configures the cache size of the central proclet to 20000:

cache size central 20000
**cache ttl**

Configures the DNS cache time to live (TTL) for positive and negative responses.

**Product**
SCM, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cache ttl { negative | positive } seconds
default cache ttl { negative | positive }
no cache { ttl { negative | positive } }
```

---

**no**
Disables any or all configured DNS cache parameters.

---

**default**
Sets the DNS cache time to live for positive and negative responses to default setting.

```
{ negative | positive } seconds
```

- **negative seconds**: Specifies the time to live for negative responses. *seconds* must be an integer value from 60 to 86400. The default value is 60 seconds.
- **positive seconds**: Specifies the time to live for positive responses. *seconds* must be an integer value from 60 to 86400. The default value is 86400 seconds (1 day).

---

**Usage**
Use this command to adjust the DNS cache time to live.

---

**Example**
The following commands set the TTL DNS cache to 90 seconds for negative responses and 43200 seconds for positive responses:

```
cache ttl negative 90

cache ttl positive 43200
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
**exit**

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
resolver

Configure the number of DNS query retries and the retransmission interval once the response timer times out.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
resolver { number-of-retries retries | retransmission-interval time }
default { number-of-retries | retransmission-interval }
```

**default**
Use this keyword to reset the specified resolver configuration to the default.

**number-of-retries retries**
Configures the number of DNS query retries on DNS response timeout.
`retries`: enter an integer from 0 to 4. Default is 2 retries.

**retransmission-interval time**
Configures the initial retransmission interval, in seconds, for retransmission after the DNS response timeout.
The retransmission interval doubles after each retry when only one server is configured. In case both primary and secondary servers are configured, the retransmission time is doubled for the last retry.
`time`: enter an integer from 2 to 5. Default is 3 seconds.

Usage
Set the DNS retransmission retries or the retransmission interval. Issue the command twice to configure both parameters, one-at-a-time.

Example
The following command sets the DNS resolver retries to 4:

```
resolver number-of-retries 4
```
round-robin answer

This command configures the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Product  SGSN
Privilege  Security Administrator, Administrator
Syntax

   [ no | default ] round-robin-answers

   no
   Removes the configured round robin method for DNS answer.

   default
   Disabled the round robin method for DNS answer.

Usage

   Use this command to configure the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Example

   The following command configures the DNS client to use round robin method for DNS query answers:

   default ] round-robin-answers
Chapter 81
EAP Authentication Configuration Mode Commands

The EAP Authentication Configuration Mode is used to configure the EAP authentication methods for the crypto template.

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

Configures shared key values for the EAP-AKA authentication method used by subscribers using this crypto template.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
eap-aka { encrypted key hex | key hex }
```

- **encrypted key hex**
  Specifies that the shared key is to be encrypted. `hex` must be a 16-character alpha and/or numeric string or a hexadecimal number beginning with “0x”.

- **key hex**
  Specifies that the shared key is to be transmitted in clear text. `hex` must be a 16-character alpha and/or numeric string or a hexadecimal number beginning with “0x”.

**Usage**
Use this command to set shared key parameters for subscribers using the EAP-AKA authentication method.

**Example**
The following command configures a clear-text shared key value for the EAP-AKA method:

```
eap-aka key aa11223344556677
```
eap-gtc

Configures shared key values for the EAP-GTC authentication method used by subscribers using this crypto template.

**Product**

PDIF, ASN GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
eap-gtc { encrypted key value | key value }
```

- **encrypted key value**
  
  Specifies that the shared key is to be encrypted. `value` must be a 16-character alpha and/or numeric string.

- **key value**
  
  Specifies that the shared key is to be transmitted in clear text. `value` must be a 16-character alpha and/or numeric string.

**Usage**

Use this command to set shared key parameters for subscribers using the EAP-GTC authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-GTC method:

```
eap-GTC key a1123344556677
```
eap-md5

Configures shared key values for the EAP-MD5 authentication method used by subscribers using this crypto template.

**Product**
PDIF, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
eap-md5 { encrypted key value | key value }
```

- **encrypted key value**
  Specifies that the shared key is to be encrypted. `value` must be a 16-character alpha and/or numeric string.

- **key value**
  Specifies that the shared key is to be transmitted in clear text. `value` must be a 16-character alpha and/or numeric string.

**Usage**
Use this command to set shared key parameters for subscribers using the EAP-MD5 authentication method.

**Example**
The following command configures a clear-text shared key value for the EAP-MD5 method:

```
eap-md5 key aa1223344556677
```
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the previous mode.
Chapter 82
EAP Configuration Mode Commands

The EAP Configuration Mode is used to configure parameters comprising an Extensible Authentication Profile used to support EAP authentication on the system.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

eap-profile seap_profile_name

EAP Profile Configuration Mode
```

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

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the previous mode.
**max-retry**

Configures the maximum number of times the system will retry communicating with another EAP device.

**Product**
PDIF, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
max-retry num
```

```
default max-retry
```

`num`
Default: 16

Specifies the number of times to retry EAP communication with another device. `num` must be an integer from 1 to 65535.

**Usage**

Use this command to set a maximum retry number for communicating with other EAP devices.

**Example**
The following command sets the maximum number of retries to **50**:

```
max-retry 50
```
mode

Configures the system as one of three types of EAP devices: authenticator pass-through, authenticator server, or peer.

Product
PDIF, ASN GW

Privilege
Security Administrator, Administrator

Syntax

mode { authenticator-pass-through | authenticator-server | peer }
default mode

default
Configures the default mode of Authenticator-pass-through.

authenticator-pass-through
Configures the system as an authenticator pass-through allowing EAP authentication to be performed by another server.
This is the default setting for this command.

authenticator-server
Configures the system as an authenticator server. This allows the system to respond to EAP requests.

peer
Configures the system as a peer device requiring it to make EAP requests of another server or pass-through device.

Usage
Use this command to configure the system to perform as one of three types of EAP devices and configure settings in an EAP mode. Entering this command results in the following prompt:
[context_name]hostname(cfg-ctx-eap-profile-mode)
#EAP Mode Configuration Mode commands are defined in the EAP Mode Configuration Mode Commands chapter.

Example
The following command configures the system to perform as an authenticator pass-through:

    mode authenticator-pass-through
Chapter 83
EAP Mode Configuration Mode Commands

The EAP Mode Configuration Mode is used to configure EAP authentication method supported by the system.

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

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Returns to the previous mode.
method

Configures the EAP method used for authentication.

Product
PDIF, ASN GW

Privilege
Security Administrator, Administrator

Syntax

```
method { eap-aka | eap-gtc | eap-md5 } [ priority num ]
```

- **eap-aka | eap-gtc | eap-md5**
  - eap-aka: Specifies that the EAP-AKA method is to be used for authentication.
  - eap-gtc: Specifies that the EAP-GTC method is to be used for authentication.
  - eap-md5: Specifies that the EAP-MD5 method is to be used for authentication.

- **priority num**
  - Specifies a priority order for a specific EAP authentication method. *num* must be an integer from 1 to 65535.

Usage

Use this command to specify the EAP authentication method(s) to use and to place multiple methods in priority order.

Example

The following command sets EAP-AKA as one of the EAP authentication methods and places it as priority of 3:

```
method eap-aka priority 3
```
Chapter 84
EDR Format Configuration Mode Commands

The EDR Format Configuration Mode enables configuring Event Detail Record (EDR) formats.

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

This command specifies the order of fields in EDRs.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
attribute attribute { [ format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } ] [ localtime ] | [ { ip | tcp } { bytes | pkts } { downlink | uplink } ] priority priority }
```

```
no attribute attribute [ priority priority ]
```

- **no**
  Removes the specified attribute.

- **attribute**
  Specifies the attribute.

**Attributes** must be one of the following:

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-called-station-id</td>
<td>Called Station ID of the mobile handling the flow.</td>
</tr>
<tr>
<td>radius-calling-station-id</td>
<td>Calling Station ID of the mobile handling the flow.</td>
</tr>
<tr>
<td>radius-fa-nas-identifier</td>
<td>RADIUS NAS identifier of Foreign Agent (FA).</td>
</tr>
<tr>
<td>radius-fa-nas-ip-address</td>
<td>RADIUS IP address of Foreign Agent (FA).</td>
</tr>
<tr>
<td>radius-nas-identifier</td>
<td>RADIUS NAS identifier.</td>
</tr>
<tr>
<td>radius-nas-ip-address</td>
<td>RADIUS NAS IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This attribute is interchangeable with sn-st16-ip-addr for the user.</td>
</tr>
<tr>
<td>radius-user-name</td>
<td>User name associated with the flow.</td>
</tr>
<tr>
<td>sn-3gpp2-always-on</td>
<td>This option is obsolete.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-bsid</td>
<td>This option is obsolete.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-esn</td>
<td>This option is obsolete.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-ip-qos</td>
<td>This option is obsolete.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sn-3gpp2-ip-technology</td>
<td>This option is obsolete. To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-release-indicator</td>
<td>This option is obsolete. To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-service-option</td>
<td>This option is obsolete. To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-session-begin</td>
<td>This option is obsolete. To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-session-continue</td>
<td>This option is obsolete. To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-acct-session-id</td>
<td>Unique session identifier for accounting.</td>
</tr>
</tbody>
</table>
### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sn-app-protocol</code></td>
<td>Application protocol for the flow. A value indicating the protocol, such as one of the following:</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_UNKNOWN = 0</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_IP=2</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_TCP=3</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_UDP=4</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_HTTP=5</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_HTTPS=6</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_FTP=7</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_FTP_CONTROL=8</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_FTP_DATA=9</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_WTP=10</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_WSP=11</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_WTP_WSP_CONNECTION_ORIENTED=12</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_WSP_CONNECTION_LESS=13</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_DNS=14</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_ICMP=15</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_POP3=16</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_SIP=17</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_SDTP=18</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_SMTP=19</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_EMAIL=20</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_MMS=21</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_FILE_TRANSFER=22</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_WWW=23</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_RTP=24</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_RTSP=25</td>
</tr>
<tr>
<td></td>
<td>- ACS_PROTO_ICMPv6=31</td>
</tr>
<tr>
<td><code>sn-cf-category-classification-used</code></td>
<td>For Category-based Content Filtering, specifies the last classification used by system for the flow, or blank if classification was never successfully performed.</td>
</tr>
<tr>
<td></td>
<td>For URL Blacklisting, specifies category of the blacklisted URL in the Blacklist database.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **sn-cf-category-flow-action** | For Category-based Content Filtering, specifies the last action taken for the flow, or blank if content filtering was never performed. Following are the possible values:  
  - allow  
  - content-insert  
  - discard  
  - redirect-url  
  - terminate-flow  
  For URL Blacklisting, specifies the last action taken for the flow, or blank if Blacklist matching was never performed. Following are the possible values:  
  - discard  
  - terminate-flow  
  - redirect-url  
  - www-reply-code-terminate-flow |
| **sn-cf-category-policy**   | Specifies the category policy identifier that was used by Category-based Content Filtering for the flow, or blank if content filtering was never attempted for the flow.                                           |
| **sn-cf-category-rating-type** | For Category-based Content Filtering, specifies the type, either “static” or “dynamic” that was last successfully performed for the flow, or blank if content filtering was never successful for the flow.  
  For URL Blacklisting, specifies “blacklisting”.                          |
| **sn-cf-category-unknown-url** | Identifier for unknown URL under content filtering action. It holds either “1” for unknown URLs or “0” for the URLs having static rating in its database.                              |
| **sn-closure-reason**       | Reason for the termination of the flow/EDR:  
  - 0: Normal end of flow  
  - 1: End of flow by handoff processing  
  - 2: Subscriber session terminated  
  - 3: Inter-chassis Session Recovery switchover  
  - 12: Completion of transaction |
| **sn-content-label**        | Identifier of text label for content-id.                                                                                                                                                                    |
| **sn-correlation-id**       | RADIUS correlation identifier.                                                                                                                                                                              |
| **sn-direction**            | Direction of the first packet for the flow. It has following values:  
  - toMobile: This value appears when direction of first packet is towards mobile node.  
  - fromMobile: This value appears when direction of first packet is towards mobile node.  
  - unknown: This value appears when the original originator of a flow can not be determined (e.g. a flow that is interrupted due to a Inter-chassis Session Recovery switchover). |
<p>| <strong>sn-duration</strong>             | Duration between the last and first packet for the record.                                                                                                                                                    |</p>
<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn-end-time [ format format ] localtime</td>
<td>Timestamp for last packet of flow in UTC.</td>
</tr>
<tr>
<td>sn-fa-correlation-id</td>
<td>Radius Correlation Identifier of the Foreign Agent (FA).</td>
</tr>
<tr>
<td>sn-fa-ip-address</td>
<td>Foreign Agent (FA) IP address</td>
</tr>
<tr>
<td>sn-filler-blank</td>
<td>Keeps attributes place blank.</td>
</tr>
<tr>
<td>sn-filler-zero</td>
<td>Fills ‘0’ for this attribute place.</td>
</tr>
<tr>
<td>sn-flow-id</td>
<td>Flow-id assigned internally by the ACS module to each flow.</td>
</tr>
<tr>
<td>sn-format-name</td>
<td>Name of the EDR/UDR format used.</td>
</tr>
<tr>
<td>sn-group-id</td>
<td>Sequence group ID of the record.</td>
</tr>
<tr>
<td>sn-ha-ip-address</td>
<td>Home Agent (HA) IP address</td>
</tr>
<tr>
<td>sn-nat-binding-timer</td>
<td>Port chunk hold timer.</td>
</tr>
<tr>
<td>sn-nat-gmt-offset</td>
<td>GMT offset of the node generating NAT bind record.</td>
</tr>
<tr>
<td>sn-nat-ip</td>
<td>NAT IP address of the port chunk.</td>
</tr>
<tr>
<td>sn-nat-last-activity-time-gmt</td>
<td>The time when the last flow in a specific NAT set of flows was seen.</td>
</tr>
<tr>
<td>sn-nat-port-block-end</td>
<td>Last port number of the port chunk.</td>
</tr>
<tr>
<td>sn-nat-port-block-start</td>
<td>Starting port number of the port chunk.</td>
</tr>
<tr>
<td>sn-nat-port-chunk-alloc-dealloc-flag</td>
<td>Indicates whether the port chunk is allocated or released.</td>
</tr>
<tr>
<td>sn-nat-port-chunk-alloc-time-gmt</td>
<td>Indicates when the port chunk was allocated.</td>
</tr>
<tr>
<td>sn-nat-port-chunk-dealloc-time-gmt</td>
<td>Indicates when the port chunk was released.</td>
</tr>
<tr>
<td>sn-nat-realm-name</td>
<td>Name of the NAT realm.</td>
</tr>
<tr>
<td>sn-nat-subscribers-per-ip-address</td>
<td>Subscriber(s) per NAT IP address.</td>
</tr>
<tr>
<td>sn-parent-protocol</td>
<td>Indicates parent protocol of flow.</td>
</tr>
<tr>
<td>sn-rulebase</td>
<td>Name of the ACS rulebase applied.</td>
</tr>
<tr>
<td>sn-sequence-no</td>
<td>Unique sequence number (per sn-sequence-group and radius-nas-ip-address) of EDR identifier and linearly increasing in EDR file.</td>
</tr>
<tr>
<td>sn-server-port</td>
<td>TCP/UDP port number of the server in a subscriber’s data flow.</td>
</tr>
<tr>
<td>sn-st16-ip-addr</td>
<td>IP address of the chassis handling this flow.</td>
</tr>
<tr>
<td>sn-start-time [ format format ] localtime</td>
<td>Timestamp for last packet of flow in UTC.</td>
</tr>
<tr>
<td>sn-subscriber-nat-flow-ip</td>
<td>NAT IP address of NAT-enabled subscriber.</td>
</tr>
</tbody>
</table>
## Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn-subscriber-nat-flow-port</td>
<td>NAT port number of NAT-enabled subscriber.</td>
</tr>
<tr>
<td>sn-subscriber-port</td>
<td>TCP/UDP port number of the Mobile handling subscriber data flow.</td>
</tr>
<tr>
<td>sn-volume-amt { ip</td>
<td>tcp } { bytes</td>
</tr>
<tr>
<td>sn-volume-dropped-amt { ip</td>
<td>tcp } { bytes</td>
</tr>
<tr>
<td>sn-volume-ip-with-rtsp-or-rtp bytes { downlink</td>
<td>priority</td>
</tr>
<tr>
<td>transaction-downlink-bytes</td>
<td>Total downlink bytes for the transaction.</td>
</tr>
<tr>
<td>transaction-downlink-packets</td>
<td>Total downlink packets for the transaction.</td>
</tr>
<tr>
<td>transaction-uplink-bytes</td>
<td>Total uplink bytes for the transaction.</td>
</tr>
<tr>
<td>transaction-uplink-packets</td>
<td>Total uplink packets for the transaction.</td>
</tr>
</tbody>
</table>

```plaintext
```

Specifies the timestamp format.

```plaintext
localtime
```

Specifies timestamps with the local time. By default, timestamps are displayed in GMT.

```plaintext
{ ip | tcp } { bytes | pkts } { downlink | uplink }
```

Specifies bytes/packets sent/received from/by mobile.

```plaintext
priority priority
```

Specifies the position priority of the value within the EDR record. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first. priority must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

## Usage

Use this command to set the attributes and priority for EDR file format. A particular field in EDR format can be entered multiple times at different priorities. While removing the EDR field using the no attribute command either you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional priority keyword.
Example
attribute radius-user-name priority 12
end

This command returns the CLI prompt to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to change to the Exec mode.
**event-label**

This command specifies an optional event ID to use in the generated billing records.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
event-label label priority priority
no event-label
```

- `no`
  Removes previously configured event label for EDR attribute.

- `label`
  Specifies event label for attribute to be used for EDR format. `label` must be an alpha and/or numeric string of 1 through 63 characters in length.

- `priority priority`
  Indicates the CSV position of event ID in EDR record. `priority` must be an integer from 1 through 65535.

**Usage**
Use this command to set the event ID and its position in EDR file format.

**Example**

```
event-label radius_csv1 priority 23
```
exit

This command exits the EDR Format Configuration mode and returns to the ACS Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
exit
```

Usage
Use this command to return to the ACS Configuration mode.
**rule-variable**

Specifies the order of fields in the EDR.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
rule-variable protocol rule priority priority [ in-quotes ]
```

```
no rule-variable protocol rule [ priority priority ]
```

```
no
```
Removes the previously configured rule variable protocol rule and/or priority for EDR attribute.

```
protocol rule
```
Specifies the rule variable for EDR format.

`protocol` must be one of the following with specified rule:

- **bearer 3gpp**: 3GPP bearer-related configuration:
  - `charging-id`
  - `imei` — Populated with IMEI/IMEISV. Only available in StarOS 8.1 and later releases
  - `rat-type` — only available in StarOS 8.1 and later releases
  - `sgsn-address` — only available in StarOS 8.1 and later releases
  - `user-location-information` — only available in StarOS 8.1 and later releases
- **bearer 3gpp2**: 3GPP2 bearer-related configuration:
  - `always-on`
  - `bsid`
  - `esn`
  - `ip-qos`
  - `ip-technology`
  - `release-indicator`
  - `service-option`
  - `session-begin`
  - `session-continue`
- **bearer ggsn-address**: GGSN bearer-related configuration:
- **dns**: Domain Name System (DNS) related configuration:
  - `answer-name`
  - `previous-state`
• query-name
• return-code
• state
• tid

• **file-transfer**: File transfer related configuration:
  • chunk-number
  • current-chunk-length
  • declared-chunk-length
  • declared-file-size
  • filename
  • previous-state
  • state
  • transferred-file-size

• **ftp**: File Transfer Protocol (FTP) related configuration:
  • client-ip-address
  • client-port
  • command name
  • connection-type
  • filename
  • pdu-length
  • pdu-type
  • previous-state
  • reply code
  • server-ip-address
  • server-port
  • session-length
  • state
  • url
  • user

• **http**: Hypertext Transport Protocol (HTTP) related configuration:
  • **attribute-in-data**—dynamic header field in application payload
  • **attribute-in-url**—dynamic header field in URL
  • content disposition
  • content length
  • content type
  • header-length
  • host
**.payload-length**

**.pdu-length**

**.previous-state**

**.referer**

**.reply code**

**.request method**

**.session-length**

**.state**

**.transaction-length**

**.transfer-encoding**

**.uri**

**.url**

**.user-agent**

**.version**

**.x-header—extension header**

**.icmp**: Internet Control Message Protocol (ICMP) related configuration:

**.code**

**.type**

**.icmpv6**: Internet Control Message Protocol Version 6 (ICMPv6) related configuration:

**.code**

**.type**

**.imap**: Internet Message Access Protocol (IMAP) related configuration:

**.cc**

**.command**

**.content**

**.date**

**.final-reply**

**.from**

**.mail-size**

**.mailbox-size**

**.message-type**

**.previous-state**

**.session-length**

**.session-previous-state**

**.session-state**

**.state**

**.subject**
IP: Internet Protocol (IP) related configuration:
  *dst-address*
  *protocol*
  *server-ip-address*
  *src-address*
  *subscriber-ip-address*
  *total-length*
  *version*

MMS: Multimedia Message Service (MMS) related configuration:
  *bcc*
  *cc*
  *content location*
  *content type*
  *date [ format { MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS } ]*
  *from*
  *message-size*
  *previous-state*
  *response status*
  *state*
  *subject*
  *tid*
  *to*

P2P protocol: Peer-to-peer protocol related configuration

POP3: Post Office Protocol version 3 (POP3) related configuration:
  *command name*
  *mail-size*
  *pdu-length*
  *pdu-type*
  *previous-state*
  *reply status*
  *session-length*
  *state*
  *user-name*

RTCP: RTP Control Protocol (RTCP) related configuration:
  *control-session-flow-id*
  *jitter*
• rtsp-id
• uri
• rtp: Real-time Transfer Protocol (RTP) related configuration:
  • control-session-flow-id
  • pdu-length
  • rtsp-id
  • session-length
  • uri
• rtsp: Real Time Streaming Protocol (RTSP) related configuration:
  • command-id
  • content type
  • date
  • previous-state
  • reply code
  • request method 1: play method
  • request method 2: setup method
  • request method 3: pause method
  • request method 4: record method
  • request method 5: options method
  • request method 6: redirect method
  • request method 7: describe method
  • request method 8: announce method
  • request method 9: teardown method
  • request method 10: get-parameter method
  • request method 11: set-parameter method
  • request packet
  • rtp-uri
  • session-id
  • session-length
  • state
  • uri
  • uri sub-part
  • user-agent
• sdp: Session Description Protocol (SDP) related configuration:
  • connection-ip-address
  • media-audio-port
  • media-video-port
• **secure-http**: HTTPS related configuration

• **sip**: Session Initiation Protocol (SIP) related configuration:
  - *call-id*
  - *content type*
  - *from*
  - *previous-state*
  - *reply code*
  - *request method*
  - *request packet*
  - *state*
  - *to*
  - *uri*
  - *uri sub-part*

• **smtp**: Simple Mail Transfer Protocol (SMTP) related configuration:
  - *command name*
  - *mail-size*
  - *pdu-length*
  - *previous-state*
  - *recipient*
  - *reply status*
  - *sender*
  - *session-length*
  - *state*

• **tcp**: Transmission Control Protocol (TCP) related configuration:
  - *dst-port*
  - *duplicate*
  - *flag*
  - *out-of-order*
  - *payload-length*
  - *previous-state*
  - *src-port*
  - *state*

• **traffic-type**: Traffic type of flow (voice or non-voice depending upon flow type).

• **udp**: User Datagram Protocol (UDP) related configuration:
  - *dst-port*
  - *src-port*
• **voip-duration**: Duration of voice call, in seconds. For a flow in which voice call end is detected, output will be a non-zero value. For other flows it will be zero.

• **wsp**: Wireless Session Protocol (WSP) related configuration
  *content type
  *host
  *pdu-length
  *pdu-type
  *reply code
  *session-length
  *tid
  *total-length
  *url
  *user-agent

• **wtp**: Wireless Transaction Protocol (WTP) related configuration
  *gtr—Group Transmission Flag
  *pdu-length
  *pdu-type
  *previous-state
  *state
  *tid
  *transaction class
  *ttr—Trailer Transmission flag

---

**Important**: For more information on protocol-based rules, see the *Ruledef Configuration Mode Commands* chapter.

```
priority priority
```

Specifies the CSV position of protocol rule related information in EDR record.

*priority* must be an integer from 1 through 65,535.

```
inquotes
```

Specifies placing double quotes (""") around the specified EDR field in the EDR.

---

**Important**: At the present time this keyword is only valid for the MMS protocol to and subject fields.

```
rule-variable mms to priority priority [in-quotes] rule-variable mms subject priority priority [in-quotes]
```

---

**Usage**

Use this command to set the rule variables priority for EDR file format.
A particular field in an EDR format can be entered multiple times at different priorities. While removing the EDR field using the `no rule-variable` command you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional `priority` keyword.

**Example**

```
rule-variable tcp dst-port priority 36
```
Chapter 85
EDR Module Configuration Mode Commands

To access the EDR Module Configuration Mode, in the Context Configuration Mode, enter the edr-module active-charging-service command.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

edr-module active-charging-service

EDR Module Configuration Mode
```

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

This command configures the EDR/UDR file parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cdr [ [ push-interval value ] [ push-trigger space-usage-percent trigger_percentage ] [ remove-file-after-transfer ] [ transfer-mode { pull | push primary { encrypted-url enc_url | url url } [ via local-context ] [ secondary { encrypted-secondary-url enc_sec_url | url sec_url } ] } ] ] + | use-harddisk ]
```

```
no cdr [ remove-file-after-transfer | use harddisk ] +
```

```
default cdr [ push-interval | push-trigger space-usage-percent | remove-file-
after-transfer | transfer-mode [ push via ] | use harddisk ] +
```

```
no
```

Disables the configured CDR storage and CDR file processing in this mode:

* **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.

* **use-harddisk**: Disables data storage on the SMC harddisk.

---

**Important**: use-harddisk keyword is only available on an ASR 5000 chassis.

**default**

Configures the default settings:

* **push-interval**: 300 seconds

* **push-trigger**: 80 percent

* **remove-file-after-transfer**: Disabled

* **transfer mode**: Pull

* **push via**: LC is used for push

* **use harddisk**: Disabled

---

**Important**: use-harddisk keyword is available only on the ASR 5000 chassis.

```
push-interval value
```

Default: 300

Specifies the transfer interval, in seconds, to push EDR and UDR files to an external file server.
value must be an integer from 60 through 3600.

\[\text{push-trigger space-usage-percent trigger_percentage}\]

Default: 80%

Specifies the EDR/UDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server.

\[\text{trigger_percentage}\] specifies the EDR/UDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.

\[\text{remove-file-after-transfer}\]

Default: Disabled

Specifies that the system must delete EDR/UDR files after they are transferred to the external file server.

\[\text{transfer-mode}\ (\text{pull} | \text{push} \ \text{primary} \ (\text{encrypted-url} \ \text{enc_url} | \text{url} \ \text{url}) \ \text{via} \ \text{local-context} \) \ [ \text{secondary} \ (\text{encrypted-secondary-url} \ \text{enc_sec_url} | \text{secondary-url} \ \text{sec_url}) \]\]

Specifies the EDR/UDR file transfer mode—how the EDR and UDR files are transferred to an external file server.

- **pull**: Specifies that the L-ESS is to pull the CDR files.
- **push**: Specifies that the system is to push CDR files to the configured L-ESS.
- **primary encrypted-url enc_url**: Specifies the primary URL location in encrypted format to which the system pushes the CDR files. **enc_url** must be the location name in an encrypted format, and must be an alpha and/or numeric string of 1 through 1024 characters in length.
- **primary url url**: Specifies the primary URL location to which the system pushes the CDR files. **url** must be an alpha and/or numeric string of 1 through 1024 characters in the //user:password@host:[port]/directory format.
- **via local-context**: Configuration to select LC/SPIO for transfer of CDRs. The system pushes the EDR files via SPIO in the local context.
- **encrypted-secondary-url enc_sec_url**: Specifies the secondary URL location in encrypted format to which the system pushes the CDR files when the primary location is unreachable or fails. **enc_sec_url** must be the location name in an encrypted format, and must be an alpha and/or numeric string of 1 through 1024 characters in length.
- **secondary-url sec_url**: Specifies the secondary URL location to which the system pushes the CDR files when the primary location is unreachable or fails. **sec_url** must be an alpha and/or numeric string of 1 through 1024 characters in //user:password@host:[port]/directory format.

\[\text{use-harddisk}\]

Default: Disabled

Specifies that on ASR 5000 chassis the hard disk on the SMC be used to store EDR/UDR files. On configuring to use the hard disk for EDR/UDR storage, EDR/UDR files are transferred from RAMFS on the PSC to the hard disk on the SMC.

\[\text{Important: use-harddisk}\] keyword is only available on ASR 5000 chassis.

+ Indicates that more than one of the previous keywords can be entered within a single command.
Usage

Use this command to configure how the charging data records (CDR) are moved and stored.
Run this command on the ASR 5000 chassis only from the local context. Running this command in any other
context will cause a failure and deliver an error message.
The use-harddisk keyword is only available on ASR 5000 chassis. This command can be run only in a
context where CDRMOD is running. Configuring in any other context will result in failure with the message
“Failure: Please Check if CDRMOD is running in this context or not.”
This config can be applied either in the EDR/UDR module, but will be applicable both to the EDR and UDR
modules. Configuring in one of the modules prevents the configuration to be done in the other module.
If PUSH transfer mode is selected, the L-ESS server URL to which the CDR files need to be transferred to
must be specified. The configuration allows a primary and a secondary server to be configured. Configuring
the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive
times, the files will be transferred to the secondary server. The transfer will switch back to the original
primary server when:
  - Four consecutive transfer failures to the secondary server occur
  - After switching from the primary server, 30 minutes elapses

When changing transfer-mode from pull to push, disable the PULL from L-ESS and then change the
transfer mode to push. Make sure that the push server URL configured is accessible from the local context.
Also, make sure that the base directory that is mentioned contains udr directory created within it.
When changing transfer-mode from push to pull, after changing, enable PULL on the L-ESS. Any of the
ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH
activity going on at the time of this configuration change, all the PUSH related configuration is nullified
immediately.

Example

The following command retains a copy of the data file after it has been transferred to the storage location:

    no cdr remove-file-after-transfer
end

This command returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
exit

This command exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
file

This command configures EDR file parameters.

Product
All

Privilege
Security Administrator, Administrator

Syntax

file [ charging-service-name { include | omit } ] [ compression { gzip | none } ] [ current-prefix string ] [ delete-timeout seconds ] [ directory dir_name ] [ edr-format-name ] [ exclude-checksum-record ] [ field-separator { hyphen | omit | underscore } ] [ file-sequence-number rulebase-seq-num ] [ headers ] [ name file_name ] [ reset-indicator ] [ rotation { num-records | number | time-segments | volume-bytes } ] [ sequence-number { length length | omit | padded | padded-sixth-length | unpadded } ] [ storage-limit limit ] [ single-edr-format ] [ time-stamp { expanded-format | rotated-format | unix-format } ] [ trailing-text string ] [ trap-on-file-delete ] [ xor-final-record ] +

default file [ charging-service-name ] [ compression ] [ current-prefix ] [ delete-timeout ] [ directory ] [ edr-format-name ] [ field-separator ] [ file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [ rotation { num-records | time | volume } ] [ sequence-number ] [ storage-limit ] [ time-stamp ] [ trailing-text ] +

default
Sets the default configuration.

charging-service-name { include | omit }
Specifies the inclusion/exclusion of charging service name in the file name.
  •include: Sets this command to include the charging service name in EDR file name.
  •omit: Sets this command to exclude the charging service name in EDR file name.

compression { gzip | none }
Specifies compression of EDR files.
  •gzip: Enables GNU zip compression of the EDR file at approximately 10:1 ratio.
  •none: Disables Gzip compression.

current-prefix string
Default: curr
Specifies a string to add to the beginning of the EDR file that is currently being used to store EDR records.
string must be an alpha and/or numeric string of 1 through 31 characters in length.

delete-timeout seconds
Default: Disabled
Specifies a time period, in seconds, when completed EDR files are deleted. By default, files are never deleted. *seconds* must be an integer from 3600 through 3153600.

**directory dir_name**
Default: /records/edr
Specifies a subdirectory in the default directory in which to store EDR files. *dir_name* must be an alpha and/or numeric string of 1 through 191 characters in length.

**edr-format-name**
Specifies creation of separate files for EDRs that have different formats. The EDR format name will be included in the file name.

**exclude-checksum-record**
Default: Disabled, inserts checksum record into the EDR file header.
When entered, this keyword excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic redundancy check (CRC) of all preceding records from the EDR file.

**field-separator [ hyphen | omit | underscore ]**
Specifies the field inclusion/exclusion type of separators between two fields of EDR file name.
- **hyphen**: Specifies the field separator as ‘-’ (hyphen) symbol between two fields.
- **omit**: Removes or omits the field separator between two fields.
- **underscore**: Specifies the field separator as ‘_’ (underscore) symbol between two fields.

**file-sequence-number rulebase-seq-num**
Specifies that the file name sequence numbers be unique per rulebase and EDR format name combination.

**headers**
Includes a file header summarizing the record layout.

**name file_name**
Default: edr
Specifies a string to be used as the base file name for EDR files. *file_name* must be an alpha and/or numeric string of 1 through 31 characters in length. The file name format is as follows:
base_rulebase_format_sequnenum_timestamp
- **base**: Specifies type of record in file or contains the operator-specified string. Default: edr
- **rulebase**: Specifies the name of the Rulebase. EDRs from different Rulebases go into different EDR files.
- **format**: Specifies the name of the EDR format if single-edr-format is specified else the format field (and the trailing underscore) is omitted from the filename.
- **sequencenum**: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all EDR files on the system.
- **timestamp**: Contains a timestamp based on file creation time in UTC time in MMDDYYYYHHMMSS format.
EDR files that have not been closed have a string added to the beginning of their filenames.
Filename for an EDR file in CSV format that contains information for rule base named rulebase1 and an EDR schema named edr_schema1 appears as follows:

```plaintext
edr_rulebase1_edr_schema1_00005_01302006143409
```

If the file name is not configured it will create files for EDRs/UDRs/FDRs (xDRs) with following template with limits to 256 characters:

```plaintext
basename_ChargSvcName_timestamp_SeqNumResetIndicator_FileSeqNumber
```

- **basename**: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ECS
- **ChargSvcName**: A system context-based configurable text string that uniquely identifies a specific context-based charging service
- **timestamp**: Date and time at the instance of file creation. Date and time in the form of “MMDDYYHHmmSS” where HH is a 24-hour value from 00-23
- **SeqNumResetIndicator**: A one byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 to 255 which is incremented by a value of 1 for the following conditions:
  - Failure of an ECS software process on an individual PSC
  - Failure of the system such that a second system takes over. (For example: a backup or standby system put in place according to Interchassis Session Recovery.)
  - File Sequence Number (FileSeqNumber) rollover from 999999999 to 0
- **FileSeqNumber**: Unique file sequence number for the file with 9 digit integer having range from 000000000 to 999999999. It is unique on each system.

File name for a closed xDR file in CSV format that contains information for ECS system `xyz_city1` and charging service name `prepaid2` with timestamp `12311969190000`, and file sequence number counter reset indicator to `002` for file sequence number `034939002` appears as follows:

```plaintext
xyz_city1_preapaid2_12311969190000_002_034939002
```

File name for a running xDR file, not closed, in CSV format that contains information for the same parameters for file sequence number `034939003` prefixed with `curr_` and appears as follows:

```plaintext
curr_xyz_city1_preapaid2_12311969190000_002_034939002
```

### reset-indicator

Specifies inclusion of the reset indicator counter value from 0 through 255 in EDR file name, and is incremented (by one) whenever any of the following conditions occur:

- an ACSMgr process fails.
- a peer chassis has taken over in compliance with our Interchassis Session Recovery feature.
- the sequence number, see `sequence-number` keyword, has rolled over to zero.

### rotation 

```plaintext
rotation { num-records number | time seconds | volume bytes }
```

Defaults:

- **num-records**: 1024
- **time**: 3600 seconds
- **volume**: 102400 bytes

Specifies when to close an EDR file and create a new one.

- **num-records**: Specifies the number of records that should be added to the file. When the number of records in the file reaches the specified value, the file is complete. `number` must be an integer 100 through 10240.
- **time**: Specifies the period of time to wait before closing the EDR file and creating a new one. `seconds` must be an integer from 30 through 86400.
volume bytes: Specifies the maximum size of the EDR file before closing it and creating a new one. bytes must be an integer from 51200 to 62914560. (Note, a higher setting may improve the compression ratio when the compression keyword is set to gzip.)

sequence-number { length length | omit | padded | padded-six-length | unpadded }
Default: padded
Specifies including/excluding sequence number in the file name.
- **length length**: Includes the sequence number with the specified length. length must be the file sequence number length with preceding zeroes in the file name, and must be an integer from 1 through 9.
- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

**Important**: The length configuration is applicable in both EDR and UDR modules. When applied in both modules without the `file udr-seq-num` configuration, the minimum among the two values will come into effect for both the modules. With the `file udr-seq-num` config, each module will use its own value of length.

single-edr-format
Default: Disabled
Creates separate files for EDRs having different formats.

storage-limit limit
Default: 33554432
Specifies deleting files when the specified amount of space, in bytes, is used up for EDR/UDR file storage on the PSC’s RAM.
On an ASR 5000 chassis, limit must be an integer from 10485760 through 536870912.

**Important**: On an ASR 5000 chassis the total storage limit is 536870912 bytes (512 MB). This limit is for both UDR and EDR files combined.

time-stamp { expanded-format | rotated-format | unix-format }
Specifies the timestamp of when the file was created be included in the file name.
- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the time stamp format to YYYYYMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of x.y, where x is the number of seconds since 1/1/1970 and y is the fractional portion of the current second that has elapsed.

trailing-text string
Specifies the inclusion of arbitrary text string in the file name.
**file**

`string` must be an alpha and/or numeric string of 1 through 30 characters in length.

**trap-on-file-delete**
Default: Disabled
This keyword instructs the system to send an SNMP notification (trap) when an EDR/UDR file is deleted due to lack of space.

**xor-final-record**
Default: Disabled
Specifies inserting an xor checksum (in place of the CRC checksum) into the EDR file header if the `exclude-checksum-record` is left at its default setting.

More than one of the previous keywords can be entered within a single command.

**Usage**
Use this command to configure EDR file characteristics.

**Example**
The following command sets the prefix of the current active EDR file to `Current`:

```
file current-prefix Current
```

The following command sets the base file name to `EDRfile`

```
file name EDRfile
```
Chapter 86

eGTP Service Configuration Mode Commands

The eGTP Service Configuration Mode is used to create and manage eGTP interface types and associated parameters.
associate

Configures an association with a GTP-U service where parameters are applied to the GTP-U data flow.

Product
P-GW

Privilege
Administrator

Syntax

associate gtpu-service name

no associate gtpu-service

no
Removes the association to the configured GTP-U service from this service.

gtpu-service name
Associates a GTP-U service with this eGTP service. name must be from 1 to 63 alpha and/or numeric characters.

Usage
Use this command to associate a GTP-U service with this eGTP service.

Example
The following command associates this eGTP service with a GTP-U service named gtpu3:

associate gtpu-service gtpu3
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax

```bash
end
```

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
gtpc

Configure the GPRS Tunneling Protocol Control (GTP-C) plane settings for this service.

Product
MME, P-GW, S-GW

Privilege
Administrator

Syntax

```
gtpc { bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } | echo-interval seconds | ip qos-dscp { forwarding_type } | max-retransmissions num | retransmission-timeout seconds }

no gtpc { bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } } | echo-interval }

default gtpc { echo-interval | ip qos-dscp | max-retransmissions | retransmission-timeout }
```

**no**
Disables or removes the configured GTP-C setting.

**default**
Resets the specified parameter to its default value.

**bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }**
Binds the service to an interface with an IPv4 address, IPv6 address or both.

**ipv4-address ipv4_address [ ipv6-address ipv6_address ]**: Binds this service to the IPv4 address of a configured interface. Optionally, bind the service to a configured interface with an IPv6 address. *ipv4_address* must be entered as a standard IPv4 address in dotted decimal notation.

**ipv6-address ipv6_address [ ipv4-address ipv4_address ]**: Binds this service to the IPv6 address of a configured interface. Optionally, bind the service to a configured interface with an IPv4 address. *ipv6_address* must be entered as a standard IPv6 address in colon-separated notation.

**echo-interval seconds**
Default: 60
Configures the duration between the sending of echo messages. *seconds* must be an integer value from 60 to 3600.

**ip qos-dscp { forwarding_type }**
Default: af11
Specifies the IP QoS DSCP per-hop behavior to be marked on the outer header of signalling packets originating from the LTE component. This is a standards-based feature (RFC 2597). The following forwarding types are supported:

- **af11**: Designates the use of Assured Forwarding 11 per-hop behavior
- **af12**: Designates the use of Assured Forwarding 12 per-hop behavior
- **af13**: Designates the use of Assured Forwarding 13 per-hop behavior
- **af21**: Designates the use of Assured Forwarding 21 per-hop behavior
- **af22**: Designates the use of Assured Forwarding 22 per-hop behavior
- **af23**: Designates the use of Assured Forwarding 23 per-hop behavior
- **af31**: Designates the use of Assured Forwarding 31 per-hop behavior
- **af32**: Designates the use of Assured Forwarding 32 per-hop behavior
- **af33**: Designates the use of Assured Forwarding 33 per-hop behavior
- **af41**: Designates the use of Assured Forwarding 41 per-hop behavior
- **af42**: Designates the use of Assured Forwarding 42 per-hop behavior
- **af43**: Designates the use of Assured Forwarding 43 per-hop behavior
- **be**: Designates the use of Best Effort forwarding per-hop behavior
- **ef**: Designates the use of Expedited Forwarding per-hop behavior typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

<table>
<thead>
<tr>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Drop</td>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
</tr>
<tr>
<td>Medium Drop</td>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
</tr>
<tr>
<td>High Drop</td>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
</tr>
</tbody>
</table>

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

**max-retransmissions num**

Default: 4

Configures the maximum number of retries for packets. *num* must be an integer from 0 through 15.

**retransmission-timeout seconds**

Default: 5

Configures the control packet (echo message) retransmission timeout in GTP, in seconds. *seconds* must be an integer value from 1 through 20.

**Usage**

Use this command to configure GTP-C settings for the current service. This interface assumes the characteristics of an S11 reference point on the S-GW or MME.

**Example**

The following command binds the service to a GTP-C interface with an IP address of 112.334.556.778:

```
gtpc bind address 112.334.556.778
```
**interface-type**

Configures the interface type used by this service.

**Product**
MME, P-GW, S-GW

**Privilege**
Administrator

**Syntax**

```
interface-type { interface-mme | interface-pgw-ingress | interface-sgsn | interface-sgw-egress | interface-sgw-ingress }
```

- **interface-mme**: Specifies that the interface has the characteristics of an eGTP MME S11 reference point to/from an S-GW.
- **interface-pgw-ingress**: Specifies that the interface has the characteristics of an eGTP P-GW S5/S8 reference point from an S-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.
- **interface-sgsn**: Specifies that the interface has the characteristics of an eGTP S-GW S4 reference point to/from an SGSN.
- **interface-sgw-egress**: Specifies that the interface has the characteristics of an eGTP S-GW S5/S8 reference point to an eGTP P-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.
- **interface-sgw-ingress**: Specifies that the interface has the characteristics of:
  - an eGTP-C S-GW S11 reference point from the MME.
  - an eGTP-U S-GW S1-U reference point from the eNodeB.

**Usage**

Use this command to specify the type of interface this service uses. By configuring this command, the interface takes on the characteristics of the selected type.

**Example**

The following command configures the interface bound to this service to maintain the characteristics of an eGTP-C S-GW S11 reference point from an MME:

```
interface-type interface-sgw-ingress
```
validation-mode

Configures the type of validation to be performed on messages received by this service.

Product
P-GW

Privilege
Administrator

Syntax

validation-mode { custom1 | standard }

default validation-mode

default

Returns the command to the default setting of standard.

{ custom1 | standard }

custom1: Specifies that the message should be validated based on a vendor-specific set of mandatory elements.
standard: Specifies that the message should be validated based on the set of mandatory elements as defined in 3GPP 29.274.

Usage

Use this command to specify the type of validation performed on messages received by this service. The information elements contained in messages have mandatory elements and conditional elements. The standard set of elements, as defined by 3GPP 29.274 is checked if this command is set to “standard”. The custom1 setting is for a vendor-specific set of mandatory elements.

Example

The flowering command sets the validation mode for incoming messages to standard:

validation-mode standard
Chapter 87
Ethernet Interface Configuration Mode Commands

The Ethernet Interface Configuration Mode is used to create and manage the IP interfaces for addresses, address resolution options, etc.

![Diagram of Ethernet Interface Configuration Mode]

- **Exec Mode**
  - `configure`
  - **Global Configuration Mode**
    - `context name`
    - **Context Configuration Mode**
      - `Interface name broadcast`
      - **Ethernet Interface Configuration Mode**
crypto-map

Applies the specified IPSec crypto-map to this interface.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

crypto-map map_name [ secondary-address sec_ip_addr ]

no

Deletes the application of the crypto map on this interface.

map_name

Specifies the name of the crypto map being applied. The name can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

secondary-address sec_ip_addr

Applies the crypto map to the secondary address for this interface that is specified by sec_ip_addr. sec_ip_addr must be specified using the standard IPv4/IPv6 notation.

Usage
In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should not be applied to interfaces. The crypto map must be configured in the same context as the interface.

Example
To apply the IPSEC crypto map named cmap1 to this interface, use the following command:

crypto-map cmap1
description

Configures the description text for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

description text

no description

no
Clears the description for the interface.

text
Specifies the descriptive text to use. text must be 0 to 79 alpha and/or numeric characters with no spaces or a quoted string of printable characters

Usage
Set the description to provide useful information on the interface’s primary function, services, end users, etc. Any information useful may be provided.

Example

description sampleInterfaceDescriptiveText
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Change the mode back to the Exec mode.
exit

Exits the interface configuration mode and returns to the context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Return to the context configuration mode.
**ip**

Configures the IP options for the current interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ip { access-group acl_name { in | out } [ priority-value ] | address ip_address ip_mask [ secondary | srp-activate ] | arp { arpa | timeout seconds } }
```

```
no ip { access-group acl_name { in | out } | address ip_address | arp { arpa | timeout } }
```

**no**

Disables and/or restores the option to the system default.

```
access-group acl_name { in | out } [ priority-value ]
```

*acl_name* specifies the access control list to be added/removed from the group. The ACL rules must be configured in the same context as the interface.

In Release 8.1 and later, *acl_name* must be an alpha and/or numeric string of 1 through 47 characters in length.

In Release 8.0 and earlier, *acl_name* must be an alpha and/or numeric string of 1 through 79 characters in length.

The direction must also be specified as either inbound or outbound using the keywords *in* and *out*, respectively.

*priority-value*: Default: 0. If more than one ACL is applied, *priority-value* specifies the priority in which they will be compared against the packet. If not specified, the priority is set to 0. *priority-value* must be an integer from 0 through 4294967295. If access groups in the list have the same priority, the last one entered is used first.

**Important**: Up to 8 ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128 rule limit for the interface.

```
address ip_address ip_mask [ secondary | srp-activate ]
```

Configures the IP address for the interface specifying the networking mask as well. *ip_address* and *ip_mask* must be specified using the standard IPv4/IPv6 notation.

The *secondary* keyword is used to configure a secondary IP address on the interface. This is referred to as multi-homing of the interface.

The *srp-activate* Activates the IP address for Interchassis Session Redundancy.
Ethernet Interface Configuration Mode Commands

## ARP Configuration

### Command Syntax

```
arp { arpa | timeout seconds }
```

### Important

These keywords have been replaced by the `arp` command in the Global Configuration Mode. For backwards compatibility, however, these keywords are accepted as valid.

### Usage

Create and manage the IP interfaces for the associated context.

### Example

The following command configures the access group for the current context:

```
ip access-group sampleAccessGroup
```

The following command sets the address resolution protocol timeout.

```
ip arp timeout 1800
```

The following commands remove the associated IP address and disable ARP for the interface, respectively.

```
no ip address 1.2.3.
no ip arp arpa
```
**ip mtu**

Configures the Maximum Transmission Unit (MTU) for this IP interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
ip mtu mtu-size

no ip mtu mtu-size
```

**Usage**

On ASR 5000 we support IP MTU with a normal interface and point-to-point interface (for OLC port). The maximum MTU size allowed with an OLC port is 1600, the maximum MTU size allowed with an Ethernet port is 2048. The default MTU size is 1500.

**Example**
The following command sets the MTU value to the default.

```
ip mtu 1500
```
ip ospf authentication-key

This command configures the password for the authentication with neighboring routers.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

- **no**
  Deletes the authentication key.

- **encrypted**
  Use this keyword if you are pasting a previously encrypted authentication key into the CLI command.

- **password auth_key**
  The password to use for authentication. `authentication_key` is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication password. This variable is entered in clear text format.

**Usage**

Use this command to set the authentication key used when authenticating with neighboring routers.

**Example**

To set the authentication key to 123abc, use the following command:

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key:

```
no ip ospf authentication-key
```
ip ospf authentication-type

This command configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ip ospf authentication-type { message-digest | null | text }
no ip ospf authentication-type { message-digest | null | text }
```

- **no**
  - Disable this function.

- **message-digest**
  - Set the OSPF authentication type to use the message digest (MD) authentication method.

- **null**
  - Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

- **text**
  - Set the OSPF authentication type to use the clear text authentication method.

**Usage**

Use this command to set the type of authentication to use when authenticating with neighboring routers.

**Example**

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```
**ip ospf cost**

This command configures the cost associated with sending a packet over the logical interface.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip ospf cost value
no ip ospf cost
```

- **no**
  - Disable this function.

- **value**
  - Default: 10
  - The cost to assign to OSPF packets. This must be an integer from 1 through 65535.

**Usage**
Use this command to set the cost associated with routes from the interface.

**Example**
Use the following command to set the cost to 20;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```
ip ospf intervals

This command configures the interval or delay type, and the interval or delay time in seconds, for OSPF communications.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

ip ospf { dead-interval value | hello-interval value | retransmit-interval value | transmit-delay value }

no ip ospf { dead-interval | hello-interval | retransmit-interval | transmit-delay }

no
Deletes the value set and returns the value to its default.

dead-interval value
Default: 40
The interval, in seconds, that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. value must be an integer from 1 through 65535.

hello-interval value
Default: 10
The interval, in seconds between sending hello packets. value must be an integer from 1 through 65535.

retransmit-interval value
Default: 5
The interval, in seconds, between LSA (Link State Advertisement) retransmissions. value must be an integer from 1 through 65535.

transmit-delay value
Default: 1
The interval, in seconds, that the router should wait before transmitting a packet. value must be an integer from 1 through 65535.

Usage
Use this command to set the intervals or delays for OSPF communications.

Example
To set the dead-interval to 100, use the following command;
ip ospf dead-interval 100
To delete the setting for the dead-interval and reset the dead-interval value to its default of 40, use the following command:

    no ip ospf dead-interval
ip ospf message-digest-key

This command enables the use of MD5-based OSPF authentication.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
ip ospf message-digest-key key_id md5 [ encrypted ] password authentication_key
no ip ospf message-digest-key key_id
```

- **no**
  Deletes the key.

- **message-digest-key key_id**
  Specifies the key identifier number. key_id must be an integer from 1 through 255.

- **encrypted**
  Use this if you are pasting a previously encrypted authentication key into the CLI command.

- **password authentication_key**
  The password to use for authentication. authentication_key is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication password. This variable is entered in clear text format.

Usage
Use this command to create an authentication key that uses MD5-based OSPF authentication.

Example
To create a key with the ID of 25 and a password of 123abc, use the following command;

```
   ip ospf message-digest-key 25 md5 password 123abc
```

To delete the same key, enter the following command;

```
   no ip ospf message-digest-key 25
```
ip ospf network

Configures the OSPF network type.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ip ospf network

no
Disable this function.

broadcast
Sets the network type to broadcast.

non-broadcast
Sets the network type to non-broadcast multi access (NBMA).

point-to-multipoint
Sets the network type to point-to-multipoint.

point-to-point
Sets the network type to point-to-point.

Usage
Use this command to specify the OSPF network type.

Example
To set the OSPF network type to broadcast, enter the following command;

ip ospf network broadcast

To disable the OSPF network type, enter the following command;

no ip ospf network
ip ospf priority

This command designates the OSPF router priority.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

ip ospf priority
no ip ospf priority

Usage
Use this command to set the OSPF router priority.

Example
To set the priority to 25, enter the following command:

    ip ospf priority 25

To disable the priority, enter the following command:

    no ip ospf priority
ipv6 access-group

Specifies the name of the ACL group to assign the interface to. You can filter for either inbound or outbound traffic.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

[no] ipv6 access-group group name { in | out } { priority-value }

**no**
Removes a previously configured access group association.

**group_name**
Specifies the name of the access group. group_name must be an alpha and/or numeric string of 1 to 79 characters.

**in**
Applies the filter to the inbound traffic.
Specify a priority_value for the access group from 0 to 4294967295. The lower values indicate a higher priority.

**out**
Applies the filter to the outbound traffic.
Specify a priority-value for the access group from 0 to 4294967295. The lower values indicate a higher priority.

**priority-value**
Default: 0
Specifies the priority of the access group. 0 is the highest priority. If priority-value is not specified the priority is set to 0. priority-value must be a value from 0 to 4294967295.
If access groups in the list have the same priority, the last one entered is used first.

Usage
Use this command to specify the ACL group to assign the interface to. Specify an ACL group name with this command.

**Important:** Up to 8 ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128 rule limit for the interface.

Example
Use the following command to associate the group_1 access group with the current IPv6 profile for inbound access:

```
ipv6 access-group group_1 in
```
ipv6 address

Specifies the address and subnet mask.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
ipv6 address ip_address

ip_address
Specifies an individual host IP address to add to this host pool.
ip_address is the IP address in colon separated notation.
```

Usage

Configures the IPv6 address and subnet mask for a specific interface.
ipv6 router advertisement

Enables or disables the system to send IPv6 router advertisements.

**Product**

PDSN, HA

**Privilege**

Security Administrator, Administrator

**Syntax**

`[no] ipv6 router advertisement`

**Usage**

Enables sending of router advertisements on the interface. All of the pool prefixes in the context (belonging to the interface) will be advertised in the router advertisement.

The router-lifetime in the advertisement is sent as 0 to indicate to the receiver that the sender cannot be a default-router. For all the prefixes (pools), the valid and preferred lifetime are sent as default. The router-advertisement is sent every 600 seconds.

If the pool-prefix is deleted, then an router-advertisement is sent for that particular prefix with the valid and preferred time set to 0.
**policy-forward**

Configure the system for redirecting the HA packets to new HA during existing HA upgradation.

**Product**

PDSN, HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
policy-forward { icmp unreachable next-hop ip address /unconnected-address next-system ip address }
```

```
no policy-forward unconnected-address
```

<table>
<thead>
<tr>
<th>no policy-forward unconnected-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes the policy forwarding configuration for unconnected address for the current interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>icmp unreachable next-hop ip address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies routing of Internet Control Message Protocol (icmp) unreachable is required in overlapping pool configuration. <code>ip address</code> must be an IP address expressed in IPv4/IPv6 notation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>unconnected-address next-system ip address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies address of next system HA to handle processing during HA upgrade. <code>ip address</code> must be an IP address expressed in IPv4/IPv6 notation.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the redirecting policy for IP packets from existing HA to new HA during upgradation. To configure this command both keyword will be in separate interface.

**Important:** It is a customer specific command.

To configure existing HA system for redirecting the HA packets to new HA during existing HA upgrade enter the following command:

```
policy-forward unconnected-address next-system ip address policy-forward icmp unreachable next-hop ip address
```
pool-share-protocol

Configure the primary or secondary system for the IP pool sharing protocol and enter IPSP configuration mode.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
pool-share-protocol { primary address | secondary address } [mode { active | inactive | check-config }]
no pool-share-protocol
```

**no pool-share-protocol**

Deletes the IP pool sharing protocol information from the current interface.

**primary address**

On the secondary system, define the IP address of an interface on the primary system that has identical IP pools configured for use with the IP pool sharing protocol. `address` must be an IP address expressed in IP v4 dotted decimal notation.

**secondary address**

On the primary system, define the IP address of an interface on the secondary system that has identical IP pools configured for use with the IP pool sharing protocol. `address` must be an IP address expressed in IP v4 dotted decimal notation.

**mode { active | inactive | check-config }**

This is an optional command to manage the mode for IP pool sharing protocol for primary or secondary HA. 

- **active**: Activates the IP pool sharing protocol mode.
- **inactive**: Inactivates the IP pool sharing protocol mode.
- **check-config**: Verify the IP pool sharing protocol configuration.

**Usage**

Use this command to set the IP address of the primary or secondary system for use with the IP pool sharing protocol and enter ipsp configuration mode. This command must be configured for an interface in each context that has IP pools configured. Refer to the System Administration and Configuration Guide for information on configuring and using the IP pool sharing protocol.

**Important:** Both the primary and secondary systems must be in the same subnet.

**Important:** For information on configuring and using IPSP refer to the System Administration and Configuration Guide.
**Important:** To reserve free addresses on primary HA for this command use reserved-free-percentage command in *IPSP Configuration Mode Commands* of this guide.

**Example**
To configure a secondary system with an IP address of 192.168.100.10 for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10
```

To inactivate a secondary system with an IP address of 192.168.100.10 for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10 mode inactive
```
port-switch-on-L3-fail

This command causes the line card port to which the current interface is bound to switch over to the port on the redundant line card when connectivity to the specified IP address is lost.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
port-switch-on-L3-fail address { ip_address | ipv6_address } [ minimum-switchover-period switch_time ] [ interval int_time ] [ timeout time_out ] [ num-retry number ]
```

```
no port-switch-on-L3-fail
```

```
no
Disable port switchover on failure.
```

```
ip_address
The IP address to monitor for connectivity. ip_address must be in either ipv4 format or IPv6 format
```

```
minimum-switchover-period switch_time
Default: 120 seconds
After a switchover occurs, another switchover cannot occur until the amount of time specified has elapsed.
switch_time must be an integer in the range from 1 to 3600.
```

```
interval int_time
Default: 60 seconds
This specifies how often, in seconds, monitoring packets are sent to the IP address being monitored.
int_time must be an integer in the range from 1 to 3600.
```

```
timeout time_out
Default: 3 seconds
This specifies how long to wait without a reply before resending monitoring packets to the IP address being monitored. time_out must be an integer in the range from 1 to 10.
```

```
um-retry number
Default: 5
This value specifies how many times to retry sending monitor packets to the IP address being monitored before performing the switchover operation. number must be an integer in the range from 1 to 100.
```

Usage
Use this command to monitor a destination in your network to test for L3 connectivity. The destination being monitored should be reachable from both the active and standby line cards.

Example
The following command enables port switchover on connectivity failure to the IP address 192.168.10.100 using default values:

```
port-switch-on-L3-fail address 192.168.10.100
```

The following command disables port switchover on connectivity failure:

```
no port-switch-on-L3-fail
```
**vlan-map**

This command sets a single next-hop IP address so that multiple vlans can use a single next-hop gateway. `vlan-map` is associated with a specific interface.

**Product**
PDSN, HA, SGSN

**Privilege**
Security Administrator, Administrator

```
vlan-map next-hop ip_address
```

**next-hop**
`ip_address`

This keyword defines an IP address for the next-hop gateway.

`ip_address`: Can be either an IPv4 or IPv6 address in standard format.

**Usage**
Use `vlan-map` to combine multiple vlan links to go through a single IP address. This feature is used in conjunction with next-hop forwarding and overlapping IP pools.
After configuring the `vlan-map`, move to the Port Ethernet configuration mode to attach the `vlan-map` to a specific vlan.

**Example**
The following command sets an IPv4 for a next-hop gateway.

```
vlan-map next-hop 123.123.123.1
```
Chapter 88
Ethernet Port Configuration Mode Commands

The Ethernet Port Configuration Mode is used to create and manage Ethernet ports and their bindings between contexts.
bind interface

Configures an association (binds) between a virtual IP interface or an SS7 or Frame Relay link to a specific context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

bind interface interface_name context_name

no bind interface interface_name context_name

Usage

Bind an interface to a context to allow the context to provide service.

Example

bind interface sampleVirtual sampleContext
no bind interface sampleVirtual sampleContext
**default**

Restores the port’s default speed and communication mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
default { medium | preferred slot | threshold { value } }
```

<table>
<thead>
<tr>
<th>medium</th>
<th>Restores the default values for the medium options as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- SPIO and fast ethernet line cards: auto</td>
<td></td>
</tr>
<tr>
<td>- Gigabit ethernet line card: auto</td>
<td></td>
</tr>
</tbody>
</table>

| preferred slot | Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port. |

<table>
<thead>
<tr>
<th>threshold { value }</th>
<th>Restores the specified port-level threshold parameter to its default value(s). The possible values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <strong>high-activity</strong>: High port activity threshold settings</td>
<td></td>
</tr>
<tr>
<td>- <strong>monitoring</strong>: Threshold monitoring configuration settings</td>
<td></td>
</tr>
<tr>
<td>- <strong>rx-utilization</strong>: Receive port utilization threshold settings</td>
<td></td>
</tr>
<tr>
<td>- <strong>tx-utilization</strong>: Transmit port utilization threshold settings</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

Restores port-level parameters to their default values.

**Example**

default medium
description

Sets the port descriptive text.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
description text

no description

no

Clears the description for the port.

text

Specifies the descriptive text to use. text must be 1 to 79 alpha and/or numeric characters with no spaces or a quoted string using printable characters.
```

**Usage**

Set the description to provide useful information on the port’s primary function, services, end users, etc. Any information useful may be provided.

**Example**

description samplePortDescriptiveText
description "This is a sample description"
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Change the mode back to the Exec mode.
exit

Exits the port configuration mode and returns to the global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the global configuration mode.
flow-control

Enables and disables flow control on the Quad Gig-E linecard (QGLC).

Product
PDSN, SGSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] flow-control

no flow-control
Disables flow control on the specified port

Usage
Flow control is enabled by default on the QGLC and can be disabled using the no command on a per-port basis. This command does not work on Fast Ethernet or Gigabit Ethernet line cards (FELC, GELC) which do not support flow control.
**Ingress-mode**

Labels this port as an ingress port.

**Product**

IPSG

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] ingress-mode
```

```
no
Disables ingress port tag.
```

**Usage**

Use this command to label this port in order for the session manager to recognize the interface from which IP data packets are being received. This command should be used in single context configurations. In single context configurations, the ingress port can only be identified if labeled.
link aggregation

Used to aggregate ports on a Quad Gig-E line card (QGLC) and set LACP parameters.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] link aggregation { master | member | group N } [ lacp { active | passive } ] [ rate { auto | slow | fast } ]
```

default link-aggregation lacp

no
This command deletes the Ethernet port from any group it might be in. If the port was the Master of a group, the whole group would be deleted.

master
This command creates the Master port for the aggregated group.
group N is an integer between 1..1023.

member
This command makes the port a member of the aggregated group.
group N is an integer between 1..1023.

lacp { active | passive }
Configures the Link Aggregation Control Protocol.
active mode sends out LACP packets periodically.
passive mode only responds to LACP packets received.

rate { auto | fast | slow }
Configures the rate at which the LACP sends packet and timeout events.
auto = the rate is controlled by the peer
fast = 1sec
slow = 30sec

default
Configures LACP default settings. Defaults are active and slow.

Usage
Configure from one to four ports on a QGLC to be in an aggregation group on the chassis to link to an aggregation group on a remote switch. Very large files can be downloaded across all ports in a group, which makes for a faster download when compared to serial downloads over a single link.
Example
The following example configures the port to be the Master for Group 2:

```
link aggregation master group 2
```
media

Configures the port interface type.

Product
All

Privilege
Security Administrator, Administrator

Syntax
media { rj45 | sfp }

rj45 | sfp
rj45: sets the physical interface to RJ-45 connectors.
sfp: sets the physical interface connection to SFP gigabit.

Usage
Set the media option when the physical cabling interface is changed.

Example
The following command sets the physical interface to RJ-45 and SFP, respectively:
media rj45
media sfp
**medium**

Configures the port speed and communication mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
medium { auto | speed { 10 | 100 | 1000 } duplex { full | half } }
```

- **auto** | **speed** { 10 | 100 | 1000 } **duplex** { full | half }

  Default: auto
  Optionally sets the speed of the interface and the communication mode.
  - auto: configures the interface to auto negotiate the interface speed.
  - speed { 10 | 100 | 1000 }: specifies the speed to use at all times.
  - duplex { full | half }: sets the communication mode of the interface to either full or half duplex.

---

**Important:** Ethernet networking rules dictate that if a device whose interface is configured to auto-negotiate is communicating with a device that is manually configured to support full duplex, the first device will negotiate to the manually configured speed of the second device but will only communicate in half duplex mode.

---

**Usage**

Set the medium options when the physical interface changes.

**Example**

The following configures the port’s speed and communication mode to be auto negotiated.

```
medium auto
```

The following command configures the port’s interface speed to gigabit with full duplex communication.

```
medium speed 1000 duplex full
```
preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery.

Default: non-revertive operation

Product

PDSN, FA, HA, SGSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

preferred slot slot#

no preferred slot slot#

Usage

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically.

Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the LC in slot 17 while ports 5 through 8 are “preferred” on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Important: This command is not supported on all platforms.

Example

preferred slot 17
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, the port is enabled with the use of the `no` keyword.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
shutdown
no shutdown
```

```
no
Enables the port. When omitted the card is shutdown (removed from service).
```

Usage
Shut down a port prior to re-cabling and/or other maintenance activities.
This command is necessary to bring a port into service by enabling it via the `no` keyword.

Example

```
shutdown
no shutdown
```


**snmp trap link-status**

Enables/disables the generation of an SNMP trap for link status changes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
snmp trap link-status
no snmp trap link-status
```

**Usage**

Enable link status change traps when a monitoring facility can use the information or if there are troubleshooting activities are in progress.

**Example**

```
snmp trap link-status
no snmp trap link-status
```
srp virtual-mac-address

Configures the SRP virtual MAC address for the port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

srp virtual-mac-address MAC_Address

no srp virtual-mac-address

Usage
The SRP virtual MAC address is applied to the port when the chassis is in SRP ACTIVE state. The default is no srp virtual-mac-address.

Important: This command is not supported on all platforms.

Example

srp virtual-mac-address MAC_Address

no srp virtual-mac-address
threshold high-activity

Configures thresholds for high port activity for the port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold high-activity high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 50
The high threshold high port activity percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thresh` can be configured to any integer value between 0 and 100.

**clear**
Allows the configuration of the low threshold.

**low_thresh**
Default: 50
The low threshold high port activity percentage that maintains a previously generated alarm condition. If the activity percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port ≥ High Threshold
- **Clear condition:** Actual percent utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

Example
The following command configures a high port utilization threshold percent of 70 and a low threshold of 50 for an
system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
threshold monitoring

Enables thresholding for port-level values.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] threshold monitoring
```

- **no**
  Disables threshold monitoring for port-level values. This is the default setting.

**Usage**

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e., high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

  The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

  “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

This command enables thresholding for port-level values. Refer to the `threshold high-activity`, `threshold rx-utilization`, and `threshold tx-utilization` commands in this chapter for
information on configuring these values. In addition refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference for information on configuring the polling interval over which these values are monitored.
threshold rx-utilization

Configures thresholds for receive port utilization.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold rx-utilization high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 80
The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

**clear**
Allows the configuration of the low threshold.

```
low_thresh
Default: 80
The low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:
- **Enter condition:** Actual percent utilization of a port for received data ≥ High Threshold
- **Clear condition:** Actual percent utilization of a port for received data < Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for a system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```
threshold tx-utilization

Configures thresholds for transmit port utilization.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold tx-utilization high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 80
The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

**clear**
Allows the configuration of the low threshold.

**low_thresh**
Default: 80
The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

**Important**: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:
- **Enter condition**: Actual percent utilization of a port for transmit data \( \geq \) High Threshold
- **Clear condition**: Actual percent utilization of a port for transmit data \( < \) Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

Example
The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```
**vlan**

Creates/deletes a VLAN tag and enters VLAN configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
vlan tag [ inline-process ] [ subscriber-vlan ] [ -noconfirm ]
```

```
novlan tag
```

- **tag**
  - A tag that you specify to identify the VLAN. The tag must be unique and not used by any other VLANs on any other ports in the system. `tag` must be an integer from 1 through 4095.

- **inline-process**
  - Do not use this keyword. This is a restricted keyword. It sets this VLAN for special processing for packets received from an external inline server.

- **subscriber-vlan**
  - Designates the VLAN type as a subscriber VLAN. This keyword must be specified if the VLAN is to be associated with specific subscribers. Refer to the `ip vlan` command in the Subscriber Configuration Mode chapter of this reference for additional information on Subscriber-VLAN associations.

**Important**: To maintain optimal performance, this keyword should not be specified for VLANs that are not to be associated with subscribers.

- **-noconfirm**
  - Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services. They are configured as “tags” on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.
**Important:** VLANs are supported in conjunction with ports on the Ethernet 10/100 and 1000 line cards and on the four-port Quad Gig-E Line Card (QGLC). (VLAN tagging is not supported for SPIO ports.) The system supports the configuration of VLANs as follows:

**Important:** Ethernet 1000 Line Card/QGLC: 1024 VLANs per card. QGLC supports 511 VLANs per port.

**Important:** Ethernet 10/100 Line Card: Maximum of 256 VLANs per port and a maximum of 1016 VLANs per Line Card. (VLANs on all the ports of a single 10/100 Line Card can not add up to more than 1016.)

**Important:** In order to change the type (using/removing the `subscriber-vlan` keyword) for VLANs that are already configured, the VLAN must first be deleted and then reconfigured as desired.

---

**Example**

The following example creates a VLAN and assign it the tag of 100:

```
  vlan 100
```
This section includes the commands `aaa test` through `crypto-group`.

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.
aaa test

This command tests AAA functionality between the system and a remote server.

Product
PDSN, HA, GGSN, SGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator

Syntax

```
aaa test { accounting username user_name | authenticate user_name password | session user_name password }
```

- **accounting username user_name**
  Tests RADIUS or GTPP accounting functionality for the specified user.
  `user_name` is the name of a user configured on the RADIUS or CFG server.

  **Important:** GTPP is used only in conjunction with the GGSN or SGSN product.

- **authenticate user_name password**
  Tests RADIUS authentication functionality for the specified user.
  `user_name` is the name of a user configured on the RADIUS server. `password` is the user’s password.

- **session user_name password**
  Tests both RADIUS authentication and RADIUS or GTPP accounting functionality for the specified user.
  `user_name` is the name of a user configured on the RADIUS server. `password` is the user’s password.

  **Important:** GTPP is used only in conjunction with the GGSN or SGSN product.

Usage
This command is used to test RADIUS-based authentication and RADIUS or GTPP accounting. This command may be useful for diagnosing problems with subscribers and access to the system and/or billing data.

Example
The following command verifies accounting for a user called user1:

```
aaa test accounting username user1
```

The following tests authentication for a user called user1 with a password of abc123:

```
aaa test authenticate user1 abc123
```
The following command will test both accounting and authentication for the user called user1 with a password of abc123:

```
   aaa test session user1 abc123
```
**active-charging service**

This command creates an active charging service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
active-charging service ecs_service_name [ -noconfirm ]
```

- `ecs_service_name`
  Specifies the active charging service name.

- `service_name`
  Must be an alpha and/or numeric string of 1 through 15 characters in length.

If the named service does not exist, it is created, and the CLI mode changes to the Active Charging Service Configuration mode wherein the service can be configured.

If the named service already exists, the CLI mode changes to the Active Charging Service Configuration mode wherein the service can be reconfigured.

- `-noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create an active charging service on the system. This command can be used directly in Exec-mode after issuing the `require active-charging` command in the Global Configuration mode. This command allows an operator (rather than security administrators and administrators) to configure the Enhanced charging service functionality only.

**Important:** Operator needs the special CLI privilege for Enhanced charging service functionality to be able to use this CLI command.

**Example**

The following command creates an active charging service named `test`:

```plaintext
active-charging service test
```
alarm

This command is used to disable the internal audible alarm on the system management card.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

alarm cutoff

Usage
Alarm cutoff disables the audible alarm. The alarm may be enabled following this command if an event within the system results in the audible alarm being enabled.

Example
alarm cutoff
autoconfirm

This command disables or enables confirmation for certain commands. This command affects the current CLI session only.

**Important:** Use the `autoconfirm` command in the Global Configuration Mode to change the behavior for all future CLI sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
autoconfirm
no autoconfirm
```

**Usage**
When `autoconfirm` is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When `autoconfirm` is disabled, the confirmation questions never appear. Disabling `autoconfirm` is active for the current session only.

By default `autoconfirm` is enabled.

**Example**
The following command enables command confirmation:

```
autoconfirm
```

The following command disables command confirmation for the duration of the current CLI session:

```
no autoconfirm
```
bulkstats force

This command is used to manage the system statistics for collection and delivery to the configured server.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

bulkstats force { gather | transfer }

| gather |
|-----------------
| Immediately collects the system statistics.

| transfer |
|-----------------
| Immediately send the currently collected statistics to the configured server.

Usage

When the current system statistics are desired immediately as opposed to the normal scheduled collection and delivery intervals issue this command.
Troubleshooting the system may require the review of statistics at times when the scheduled delivery is not timely.

Example

The following causes the chassis to immediately collect system statistics. This would be in anticipation of a transfer command.

bulkstats force gather

The following command causes the chassis to immediately send all collected statistics to the configured server.

bulkstats force transfer
card halt

This command halts a card. A card reboot must be issued to bring the card back into service after it is halted.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
card haltslot_num [ -force ] [ -noconfirm ]
```

- **slot_num**
  Indicates the slot number of the card of interest.

- **-force**
  Over-rides any warnings to force the card to be halted.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Halt a card to stop the card for maintenance or emergency situations.

⚠️ **Caution:** Caution should be taken in using this command as halting a card which has no redundancy card available may cause a service interruption and loss of active sessions.

⚠️ **Caution:** The `-force` and `-noconfirm` options should only be used concurrently by experienced users as this will cause an immediate halt regardless of warnings and no confirmation from the user.

ℹ️ **Important:** This command is not supported on all platforms.

Example

The following command temporarily stops the card in slot 1.

```
card halt 1
```

The following commands force the card to halt and indicate no confirmation is to take place, respectively.

```
card halt 17 -force -noconfirm
```
card lc switch

This is the command for managing the line cards and their active/standby status.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
card lc switch to target_slot [ -noconfirm ]
```

- `switch to target_slot`
  Indicates the card which is to become the active card specified as `target_slot`.

- `-noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Line card switch overs change the active/standby status of a line card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

⚠️ **Caution:** Caution should be taken in using this command. Depending on the amount of bandwidth/traffic being switched, some subscribers may experience service interruptions.

ℹ️ **Important:** This command is not supported on all platforms.

Example

The following command switches the active/standby status of the line cards where one of the cards is in slot 17. This command only executes after the user provides confirmation of the request.

```
card lc switch to 17
```

The following switches the active/standby status of the line cards where one of the cards is in slot 17. This command executes immediately with no additional user confirmation.

```
card lc switch to 17 -noconfirm
```
card lc upgrade

This command upgrades the programmables on the line card.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
card lc upgrade slot_number
```

Upgrades programmables on the specified card. Must be followed by a slot number of card to upgrade.

⚠️ **Caution:** This command should only be used if instructed by or working with Technical Support.

**Usage**
This command upgrades the linear flash on the line card.

⚠️ **Important:** This command is not supported on all platforms.

**Example**
The following command initiates a lc upgrade:

```
card lc upgrade
```
card psc

This command moves processes from the source PSC to the destination PSC or disables the PSC from accepting any new calls.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
card psc { migratefrom src_slot to dst_slot | busy-out } [ -noconfirm ]
```

```
no card psc busy-out
```

- **no card psc busy-out**
  Disable busy-out. The PSC is re-enabled to accept new calls.

- **migrate from src_slot to dst_slot**
  This keyword moves processes from the specified source PSC to the specified destination PSC. The command prompt is returned once the command is initiated. The card migration is completed in background.

  *src_slot* indicates the source slot number of the card whose processes will be migrated from.

  *dst_slot* indicates the destination slot number of the card processes will be migrated to.

- **busy-out**
  When busy-out is enabled on a PSC, the PSC stops receiving new calls but continues to process calls it currently has until they are completed. The command prompt is returned once the command is initiated. The busy-out procedure is completed in background.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Migrating a packet accelerator card changes the active/standby status of a packet accelerator card. This results in the active sessions/processes being moved to the newly active PSC. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

The destination slot specified must contain a packet accelerator card which is in the standby state for the command to complete successfully.

⚠️ **Caution**: Caution should be taken in using this command. Depending on the number of active sessions being migrated, some subscribers may experience service interruptions.

Using busy-out to refuse new calls on a PSC allows you to take a card out of service without any interruptions to the end user. An individual system can be taken completely out of service gracefully by
enabling busy-out on all PSCs and waiting for current calls to complete. The `show card` info command shows if busy-out is enabled.

**Important:** When a PSC fails, is migrated, or is restarted for any reason busy-out is reset to disabled, the default behavior.

**Important:** This command is not supported on all platforms.

**Example**
The following command migrates the active processes from the PSC card in slot 12 to the card in slot 14. This command only executes after the user provides confirmation of the request.

```plaintext
card psc migrate from 12 to 14
```

The following command sets the PSC in slot 1 to stop accepting new calls:

```plaintext
card psc busy-out 1
```
card psc upgrade

This command upgrades the programmables on the PSC card.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
card psc upgradeslot_number
```

- `upgrade`
  Upgrades programmables on the specified card. Must be followed by a slot number of card to upgrade.

⚠️ **Caution:** This command should only be used if instructed by or working with Technical Support.

Usage
You can only initiate an upgrade if:
- there is no migration occurring
- the card is active or standby
- there is no online upgrade in progress

⚠️ **Important:** The following operations are not allowed while a card is upgrading:
- change pac edc requirement
- change card [no] shutdown
- change card active
- change card redundancy
- card halt
- card reboot
- start an online upgrade

⚠️ **Important:** Level unlock operations are ignored while a card is upgrading.

⚠️ **Important:** This command is not supported on all platforms.

Example
The following command initiates a PSC upgrade:

```
card psc upgrade
```
card reboot

This performs a reset of the target card. Rebooting a packet processing or line card will result in the card downloading the image from the system management card.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
card reboot target_slot [ -force ] [ -noconfirm ]
```

- **target_slot**
  Indicates the slot number of the card which is the target of the reboot.

- **-force**
  Indicates the reboot is to take place ignoring any state or usage warnings that might be generated.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
A reboot is used to reset the card and receive a new download. This may be useful when a card is not responding or when it is necessary to cause the card to reload its image and restart.

**Important:** Caution should be taken in using this command as rebooting a card which has no redundancy card available may cause a service interruption and loss of active sessions.

**Caution:** The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate reboot regardless of warnings and no confirmation from the user.

**Important:** This command is not supported on all platforms.

Example
The following will cause the card in slot \( \theta \) to reboot without any confirmation from the user. The card will not reboot if there are any warnings generated.

```
card reboot \( \theta \) -noconfirm
```

The following command will cause the card in slot \( \theta \) to reboot regardless of any warnings. The user must provide confirmation prior to this command executing.
card reboot 8 -force

The following command will cause the card in slot 8 to reboot regardless of any warnings with no additional user confirmation.

card reboot 8 -force -noconfirm
card restart

This performs a soft-reset of the target card causing all application processes to restart.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
card restart target_slot [ -force ] [ -noconfirm ]
```

- `target_slot`
  Indicates the slot number of the card which is the target of the restart.

- `-force`
  Indicates the restart is to take place ignoring any state or usage warnings that might be generated.

- `-noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Restarting a card may be useful when a card is not performing as expected (performance drop, increased response delays, etc.). A restart may be preferred to a reboot as the card becomes available in less time than a reboot.

When this command is issued for an active card, the user is prompted for confirmation unless the `-force` and/or `-noconfirm` keywords are used. Because the reboot of standby or redundant cards is non-service impacting, the reboot proceeds immediately after the command execution without user confirmation.

**Important:** Caution should be taken in using this command as restarting a card which has no redundant card available may cause a service interruption and loss of active sessions.

**Important:** This command is not supported on all platforms.

**Caution:** The `-force` and `-noconfirm` options should only be used concurrently by experienced users as this will cause an immediate restart regardless of warnings and no confirmation from the user.

Example

The following will cause the card in slot 8 to restart without any confirmation from the user. The card will not reboot if there are any warnings generated.

```
card restart 8 -noconfirm
```
The following command will cause the card in slot 8 to restart regardless of any warnings. The user must provide confirmation prior to this command executing.

```
card restart 8 -force
```

The following command will cause the card in slot 8 to restart regardless of any warnings with no additional user confirmation.

```
card restart 8 -force -noconfirm
```
card smc

This is command is for managing the switch processor cards and their active/standby status and synchronizing the filesystem between the active device and the standby device.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

cardsmc { switchover | synchronize filesystem [ /flash | /hd | /pcmcia1 | all ] [ checkonly ] [ reverse ] } [ -noconfirm ]

- noconfirm
Executes the command without any additional prompt and confirmation from the user.

switchover
Switches control from the active SMC to the defined standby SMC.

synchronize filesystem [ /flash | /hd | /pcmcia1 | all ] [ checkonly ] [ reverse ]

/flash: Synchronizes only the filesystem on the standby SMC’s /flash device.
/hd: Synchronizes only the filesystem on the standby SMC’s hard drive.
/pcmcia1: Synchronizes only the filesystem on the standby SMC’s /pcmcia1 device.
all: Synchronizes file systems on all available matching local devices (/flash, /pcmcia1).
checkonly: Displays a list of files that could be synchronized, without executing any synchronization actions.
reverse: When used, the specified operation is performed from the standby SMC to the active SMC.

Usage
The switch over of an SMC changes the active/standby status of an SMC card. This is useful when there is a maintenance activity on the active card which requires removing the card from service. Each SMC contains independent local devices, namely a CompactFlash (/flash) and a PCMCIA card slot (/pcmcia1). Either of these devices may contain system files such as binary software images, configuration text files, boot system files, and others used to control and manage the system. This command allows the files contained on the active (currently managed) SMC to be synchronized, or mirrored, on the like local device(s) contained on the standby SMC.

Important: Only filesystems on matching local devices are synchronized. For example, if the active SMC contains two local devices (/flash and /pcmcia1) and the standby SMC contains only one local device (/flash), then synchronization only occurs on the matching local device (i.e. /flash).

Important: This command is not supported on all platforms.
Example
The following command switches the active/standby status of the switch processor cards. This command only executes after the user provides confirmation of the request:

```
card smc switchover
```

The following command switches the active/standby status of the SMCs and executes immediately with no additional user confirmation:

```
card smc switchover -noconfirm
```

The following command synchronizes the filesystems on all available matching local devices (/flash, /pcmcia1):

```
card smc synchronize filesystem all
```

The following command checks to see what files could be synchronized but no synchronization is performed:

```
card smc synchronize filesystem checkonly
```
card smc upgrade

This command updates the programmables on the SMC.

Product

All

Privilege

Security Administrator, Administrator

Syntax

card smc upgrade slot_number

upgrade

Upgrades programmables on the specified card. Must be followed by a slot number of card to upgrade.

⚠️ Caution: This command should only be used if instructed by or working with Technical Support.

Usage

You can only initiate an upgrade if:

- there is no migration occurring
- the card is active or standby
- there is no online upgrade in progress

❗️ Important: The following operations are not allowed while a card is upgrading: change pac edc requirement (config) change card [no] shutdown (config) change card active (config) change card redundancy (config) card halt (exec) card reboot (exec) start an online upgrade

❗️ Important: Level unlock operations are ignored while a card is upgrading.

❗️ Important: This command is not supported on all platforms.

Example

The following command initiates a PSC upgrade:

    card psc upgrade

⚠️ Caution: This command should only be used if instructed by or working with Technical Support.
card spio

This is the command for managing the switch processor I/O cards and their active/standby status.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

card spio switch toslot# [ -noconfirm ]

slot#
The slot number of the SPIO card that you want to switch to be the active card. The currently active SPIO card is put in standby mode and the SPIO card in the specified slot number is made active.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Switch over changes the active/standby status of a SPIO card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

Important: This command is not supported on all platforms.

Example
The following command switches the active/standby status of the switch processor I/O cards. This command only executes after the user provides confirmation of the request.

    card spio switch

The following switches the active/standby status of the switch processor I/O cards. This command executes immediately with no additional user confirmation.

    card lc switch -noconfirm
**cdr-push**

This command initiates manual push of CDR files to L-ESS.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
cdr-push { all | local-filename file_name }
```

- **all**
  Specifies to push all CDR files to the configured URL.

- **local-filename file_name**
  Specifies to push the specified file to the configured URL.
  `file_name` must be the absolute path of local file name to push, and must be a string of 1 through 1023 characters in length.

**Usage**

Use this command to manually push CDR files to the configured L-ESS.
For information on configuring the L-ESS, see the `cdr` command in the EDR Module Configuration Mode Commands/UDR Module Configuration Mode Commands chapters.
On ASR 5000 chassis, run this command only from the local context. If you are in any other context, you will see this failure message: “Failure: Manual PUSH of CDRs supported only in the local context”

**Example**
The following command pushes all CDR files to the URL:

```
cdr-push all
```
clear

The following commands clear a variety of items including statistics, conditions, alarms, sessions, and files:
**clear aaa**

This command is used to clear all AAA statistics in the current context.

**Product**
PDSN, GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear aaa local counters
```

**Usage**
Clearing the AAA statistics which may be useful when monitoring the statistics manually. Clearing resets the counters to zero.

The keyword `local` is not intended to imply the local context defined for all systems. Rather, the keyword `local` indicates the statistics within the current context are to be cleared.

**Example**
The following command zeroes out all the AAA statistics in the current context.

```
clear aaa local counters
```
clear active-charging analyzer statistics

This command is used to clear protocol analyzer statistics.

**Product**
ECS

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]
```

- `name protocol_name`
  
  Clears statistics for the specified protocol analyzer.
  
  If this keyword is not specified all statistics are cleared.
  
  `protocol_name` must be one of the following:
  
  - `dns`
  - `file-transfer`
  - `ftp`
  - `http`
  - `icmp`
  - `icmpv6`
  - `imap`
  - `ip`
  - `ipv6`
  - `mms`
  - `p2p [ application ]`: Peer-to-peer analyzer. The supported applications are:
    
    - `actsync`
    - `aimini`
    - `applejuice`
    - `ares`
    - `battlefld`
    - `bittorrent`
    - `ddlink`
    - `directconnect`
    - `edonkey`
    - `fasttrack`
    - `feidian`
    - `filetopia`
clear active-charging analyzer statistics

• freenet
• fring
• gadu_gadu
• gnutella
• halflife2
• hamachivpn
• iax
• imesh
• iptv
• irc
• iskoot
• jabber
• manolito
• msn
• mute
• nimbuzz
• openft
• orb
• oscar
• paltalk
• pando
• pandora
• popo
• pplive
• ppstream
• qq
• qqqgame
• qqlive
• quake
• rdp
• secondlife
• skinny
• skype
• slingbox
• sopcast
• soulseek
• steam
clear active-charging analyzer statistics

- tvants
- tvuplayer
- uusee
- vpnx
- vtun
- warcft3
- winmx
- winny
- wofwarcraft
- xbox
- yahoo
- zattoo

*pop3
*pptp
*rtcp
*rtp
*rtsp
*sdp
*secure-http
*sip
*smtp
*tcp
*tftp
*udp
*wsp
*wtp

grep grep_options | more

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

**Usage**

Use this command to clear active charging analyzers.

**Example**

The following command clears active charging service analyzer information for analyzer named tcp:
clear active-charging analyzer statistics name tcp
clear active-charging charging-action statistics

This command is used to clear charging action statistics.

Product
ECS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging charging-action statistics [ name<string> ] [ | {
grep grep_options | more } ]
```

- **name string**
  Clears detailed information for specific protocol analyzer.
  `<string>` must be the name of an existing charging action.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to clear active charging action statistics.

Example
The following command clears active charging action statistics information for charging action named `pre-paid`:

```
clear active-charging charging-action statistics name pre-paid
```
clear active-charging content-filtering category statistics

This command is used to clear category-based content filtering statistics for the specified rulebase.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear active-charging content-filtering category statistics [ rulebase name=rulebase_name| all ] [ | { grep|grep_options| more } ]
```

- `all`:
  Clears the statistics of each and every configured rulebase.

- `rulebase_name`:
  `rulebase_name` must be the name of an existing rulebase, and must be an alpha and/or numeric string of 1 through 15 characters in length.

- `grep grep_options | more`:
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

**Usage**
Use this command to category-based content filtering statistics.

**Example**
The following command clears category-based content filtering statistics information for Rulebase named `cf_rule1`:

```
clear active-charging content-filtering category statistics rulebase name cf_rule1
```
clear active-charging credit-control statistics

This command clears credit control statistics.

Product
ECS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging credit-control statistics [ group group_name]
```

**group group_name**
Clears statistics for the specified credit control group. *group_name* must be the name of a credit control group, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage
Use this command to clear credit control statistics.

Example
The following command clears statistics information for credit control:

```
clear active-charging credit-control statistics
```
clear active-charging edr-format statistics

Clears the statistics for the specified EDR format.

Product
ECS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging edr-format statistics [ name edr_format ]
```

- `name edr_format`
  Specifies name of the EDR format for which you want to clear the statistics.
  `edr_format` must be the name of a configured EDR format, and must be an alpha and/or numeric string of 1 through 63 characters in length.

**Important:** If an EDR format name is not specified statistics for all EDR formats are cleared.

Usage
Use this command to clear the accumulated statistics for the specified EDR format.

Example
The following command clears the statistics for all EDR formats:

```
clear active-charging edr-format statistics
```
clear active-charging edr-udr-file statistics

This command is used to clear EDR/UDR file related statistics.

Product
ECS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging edr-udr-file statistics
```

Usage

Use this command to clear EDR and UDR file statistics.

Example

The following command clears statistical information for EDR and UDR files:

```
clear active-charging edr-udr-file statistics
```
clear active-charging firewall statistics

This command clears Active Charging Stateful Firewall statistics.

**Product**
FW

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
clear active-charging firewall statistics [ callid call_id | domain-name domain_name | nat-realm nat_realm | protocol { icmp | ip | other | tcp | udp } | username user_name | [ acsmgr instance instance_id ] [ grep|grep_options | more ] ]
```

---

**acsmgr instance instance_id**

Specifies an ACS Manager instance ID.
`instance_id` must be an integer from 1 through 65535.

---

**callid call_id**

Specifies a Call Identification number.
`call_id` must be an eight-digit HEX number.

---

**domain-name domain_name**

Specifies a domain name for the statistics.
`domain_name` must be a string of 1 through 127 characters in length.

---

**nat-realm nat_realm**

Specifies a NAT realm name for the statistics.
`nat_realm` must be a string of 1 through 31 characters in length.

---

**protocol { icmp | ip | other | tcp | udp }**

Specifies protocol for the stats.
- **icmp**: ICMP protocol
- **ip**: IP protocol
- **other**: Protocols other than TCP, UDP, and ICMP
- **tcp**: TCP protocol
- **udp**: UDP protocol

---

**username user_name**

Specifies a user name for the statistics.
`user_name` must be a string of 1 through 127 characters in length.
Clear Active-Charging Stateful Firewall Statistics

```
   clear active-charging firewall statistics
```

Usage

Use this command to clear Active Charging Stateful Firewall statistics.

Example

The following command clears all Stateful Firewall statistics:

```
   clear active-charging firewall statistics
```
clear active-charging firewall track-list

This command clears the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

**Product**
FW

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
clear active-charging firewall track-list attacking-servers
```

**Usage**
Use this command to clear the list of servers being tracked for involvement in any DOS attacks.

**Example**
The following command clears the list of servers being tracked for involvement in any DOS attacks:
```
clear active-charging firewall track-list attacking-servers
```
clear active-charging fw-and-nat policy statistics

This command clears statistics for all or a specific firewall-and-NAT policy.

**Product**
FW, NAT

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear active-charging fw-and-nat policy statistics { all | name policy_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all firewall-and-NAT policies configured.

- **name policy_name**
  Displays information for the specified firewall-and-NAT policy. `policy_name` must be the name of a firewall-and-NAT policy, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
Use this command to clear statistics for all or a specific firewall-and-NAT policy.

**Example**
The following command clears statistics for the firewall-and-NAT policy named `test123`:

```
clear active-charging fw-and-nat policy statistics name test123
```
clear active-charging group-of-ruledefs statistics

This command clears statistical information related to Active Charging Service group of ruledefs.

Product
ECS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging group-of-ruledefs statistics [ name group_of_ruledefs ] [ | { grep grep_options | more } ]
```

```
name group_of_ruledefs
```
Specifies name of the group of ruledefs for which statistics must be cleared. `group_of_ruledefs` must be the name of an existing group of ruledefs, and must be a string of 1 through 63 characters in length.

```
grep grep_options | more
```
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to clear statistical information related to all or specified Active Charging Service group of ruledefs.

Example
The following command clears statistical information related to the group of ruledefs named `ruledef_group12`:

```
clear active-charging group-of-ruledefs statistics name ruledef_group12
```
clear active-charging nat statistics

This command clears NAT realm statistics.

**Product**
NAT

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear active-charging nat statistics [ nat-realm nat_realm ] [ | { grep grep_options | more } ]
```

- **clear active-charging nat statistics**
  This command when issued in the local context clears statistics for all NAT realms in all contexts. When issued in a specific context, this command clears statistics for all NAT realms in that context.

- **clear active-charging nat statistics nat-realm nat_realm**
  This command when issued in the local context clears statistics for the specified NAT realm in all contexts. When issued in a specific context, this command clears statistics for the specified NAT realm in that context.

- **nat-realm nat_realm**
  Specifies the NAT realm’s name.
  `nat_realm` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **grep grep_options | more**
  Specifies that the command’s output be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section in the Command Line Interface Reference.

**Usage**
Use this command to clear NAT realm statistics.

**Example**
The following command when issued in the local context, clears NAT realm statistics for NAT realms named `test135` in all contexts:

```
clear active-charging nat statistics nat-realm test135
```
clear active-charging rulebase statistics

This command clears ACS rulebase statistics.

Product
ECS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging rulebase statistics [ name rulebase_name ] [ | { grep grep_options | more } ]
```

- `rulebase_name`
  Clears statistics for specified ACS rulebase.
  `-rulebase_name` must be the name of an existing rulebase, and must be an alpha and/or numeric string of 1 through 15 characters in length.

- `grep grep_options | more`
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to clear ACS rulebase statistics.

Example
The following command clears statistics for the ACS rulebase named `postpaid`:

```
clear active-charging rulebase statistics name postpaid
```
clear active-charging ruledef statistics

This command clears ACS rule definition statistics.

Product
ECS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging ruledef statistics [ charging | firewall | name
ruledef_name ] [ | { grep grep_options | more } ]
```

- **charging**
  Clears statistics for all Charging rule definitions configured.

- **firewall**
  Clears statistics for all Firewall rule definitions configured.

- **name ruledef_name**
  Clears statistics for the specified active charging service rule definition.
  `ruledef_name` must be the name of an existing rule definition, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage

Use this command to clear ACS ruledef statistics.

Example

The following command clears all ruledef statistics:

```
clear active-charging ruledef statistics
```
clear active-charging subsystem

This command is used to clear all Active Charging service information.

**Product**

ECS

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
clear active-charging subsystem
```

**Usage**

Use this command to clear all Active Charging subsystem information.

**Example**

The following command clears all Active Charging service information:

```
clear active-charging subsystem
```
clear active-charging url-blacklisting statistics

This command clears URL Blacklisting feature related statistics.

Product
CF

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear active-charging url-blacklisting statistics [ rulebase name rulebase_name ] [ [ | { grep grep_options | more } ] ]
```

```
rulebase name rulebase_name
Cleans URL Blacklisting information for the specified rulebase.
rulebase_name must be the name of a rulebase, and must be a string of 1 through 63 characters in length.
```

```
grep grep_options | more
Specifies that the output of the command must be piped (sent) to the command specified. A command to send
the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the
Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.
```

Usage
Use this command to clear URL Blacklisting feature related statistics, optionally for a specific rulebase.

Example
The following command clears URL Blacklisting feature related statistics for rulebase12:

```
clear active-charging url-blacklisting statistics rulebase name rulebase12
```

clear administrator

This command ends the session of an administrative user specified by either user name or session ID.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
clear administrator { name user_name | session id id_num }
```

- **name user_name**
  Identifies the user name of the administrative user.

- **session id id_num**
  Identifies the ID number of the administrative user session as displayed in the `show administrators session id` command output.

Usage
This command is used to terminate command line interface sessions for other administrative users.

Example
The following command ends the session of the administrative user identified as user1:

```
clear administrator name user1
```

The following command ends the session of the administrative user with the session ID of 3:

```
clear administrator session id 3
```
clear alarm

Clears outstanding alarm conditions

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear alarm { all | chassis | idnum | port slot/port | slot slot }
```

- **all**
  Clear all outstanding alarms

- **chassis**
  Clears chassis-wide and fan tray alarms

- **id num**
  Clears a specific alarm by its internal alarm ID. `num` is the internal alarm identification number.

- **port slot/port**
  Clears alarms for the specified port. `slot/port` is the port to clear alarms for. `slot` is the slot that the card is installed in and `port` is the port on that card.

- **slot slot**
  Clears alarms for the specified slot. `slot` is the slot to clear alarms for.

Usage

Use this command to clear outstanding alarm conditions.

Example

To clear all outstanding alarms, use the following command:

```
clear alarm all
```

To clear all alarms for slot 7, enter the following command:

```
clear alarm slot 7
```
clear asngw-service

This command clears the service session statistics of an ASN GW service specified by either service name or trusted peer address.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
clear asngw-service statistics [name svc_name] peer-address ip_address
```

- **name svc_name**
  Identifies the name of the ASN GW service to clear all service statistics.

- **peer-address ip_address**
  Identifies the IP address of the ASN GW peer to clear all service statistics.

Usage
This command is used to terminate command line interface sessions for ASN GW services.

Example
The following command clears the service session statistics of ASN GW service named as asngw-service:

```
clear asngw-service statistics name asn_svc1
```
clear asnpc-service

This command clears the service session statistics of an ASN paging controller service specified by either ASN PC service name or trusted paging controller peer address.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
clear asnpc-service statistics [name svc_name | peer-address ip_address]
```

- **name svc_name**
  Identifies the name of the ASN PC service to clear all service session statistics.

- **peer-address ip_address**
  Identifies the IP address of the ASN PC peer to clear all service statistics.

Usage

This command is used to terminate command line interface sessions for ASN PC services.

Example

The following command clears the service session statistics of ASN PC service named as asnp_svc1:

```plaintext
clear asnpc-service statistics name asnp_svc1
```
clear apn statistics

Deletes all previously gathered statistics for either a specific APN or all APNs configured with the given context.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

clear apn statistics [ name=apn_name ]

name apn_name

Specifies the name of a specific APN configured in the context for which to clear statistics.

apn_name is the name of the APN and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Usage
Statistics for a single APN can be cleared using the name keyword. Statistics for all APNs in the context can be deleted by entering the command with no keywords.

If this command is executed from within the local context with no keywords, statistics will be cleared for every APN configured on the system regardless of context. In addition, if the name keyword is used when executing from within the local context, statistics for all APNs configured with the specified name will be cleared regardless of context.

Example
The following command clears statistics for an apn called isp1:

clear apn statistics isp1
clear bcmcs statistics

Clears BCMCS statistics.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear bcmcs statistics [ pdsn-service service_name ]
```

<table>
<thead>
<tr>
<th>pdsn-service service_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines a specific PDSN service for which to clear BCMCS-specific statistics. This value must be a string consisting of up to 63 characters.</td>
</tr>
</tbody>
</table>

Usage

Use this command to clear accumulated BCMCS statistics. You may specify an individual PDSN or peer to selectively clear statistics.

Example

```
clear bcmcs statistics
clear bcmcs statistics pdsn-service service_name
```
clear blacklisted-gtpu-bind-address

Clears the GTP-U loopback address blacklisted by a specific RNC as defined for a specific IuPS Service configuration.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear blacklisted-gtpu-bind-address ip_address rnc-id rnc-id mcc mcc_num mnc mnc_num iups-service name

**ip_address**

Specifies the IP loopback address that has been blacklisted. This loopback address was originally defined with the **associate-gtpu-bind-address** command in the Radio-Network-Controller configuration mode of the IuPS Service.

*ip_address* must be specified using the standard IPv4 dotted decimal notation.

Usage

This command enables this loopback address to be used for future RAB-assignment requests.

Example

clear blacklisted-gtpu-bind-address 1.1.1.1 rnc-id 2 mcc 123 mnc 321 iups-service iups1
clear bssap+ statistics

Clears/deletes the statistics for Base Station System Application Part plus in a Gs service sessions.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
clear bssap+ statistics [ gs-service gs_svc_name ] [ vlr { name vlr_name | isdn-number E164_ISDN_Num } ]
```

- **gs-service gs_svc_name**
  Specifies the name of a specific Gs service to clear the BSSAP+ information.
  `gs_svc_name` is the name of a configured Gs service for which BSSAP+ is applied and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **vlr { name vlr_name | isdn-number E164_ISDN_Num }**
  Specifies the name of the VLR or SS7 address in E.164 ISDN format to clear the BSSAP+ information.
  `vlr_name` is name of the VLR must be an alpha and/or numeric string of 1 to 63 characters.
  `E164_VLR_num` is an ISDN number for VLR per E.164 number plan and must be an numerical string of 1 to 15 digits.

**Usage**
Use this command to delete or clear the statistics of BSSAP+ application on a system.

**Example**
The following command clears the information about BSSAP+ in a Gs service named `gssvc1`.

```
clear bssap+ statistics gs-service gssvc1
```
clear bulkstats

Clears counters and accumulated bulk statistics related information.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
clear bulkstats { counters | data }
```

- **counters**
  Clears the counters maintained by the system’s “bulkstats” facility.

- **data**
  Clears any accumulated data that has not been transferred. This includes any “completed” files that haven't been successfully transferred.

**Usage**

Once bulk statistics collection is enabled, the system stores the information until the specified transfer criteria is met or until a manual transfer is initiated. The system maintains counters for the “bulkstats” software facility. (Refer to the **data** keyword for the **show bulkstats** command for information on viewing the counters.)

This command can be used to delete bulk statistics information that has been collected but not transferred and/or to clear the counters that have been maintained.

**Example**
The following command clears bulk statistics-related counters:

```plaintext
clear bulkstats counters
```
clear config

This command replaces the active configuration source file with an empty configuration where possible.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
clear config [ -noconfirm ]
```

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**
Clear the current configuration when a complete over write is desired or if it is necessary to start from an empty configuration.

**Important:** Clearing the configuration will cause the active configuration source file to be empty and of no use in configuring the system to an active state providing service.

**Important:** It is suggested that this command only be performed on configurations which have been backed up for easy restoration.

**Example**
The following command clears the active configuration after the user provides confirmation of the request.

```
clear config
```

The following command clears the active configuration source file immediately with no user confirmation.

```
clear config -noconfirm
```
clear congestion-control statistics

Clears the congestion control statistics for all instances of the specified manager type.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clearcongestion-controlstatistics { allmgr | asngwmgm | asnpcmgr | hamgr | gtpcmgr | 12tpmgr | imsimgr }
```

- **allmgr**
  Clears the statistics for all A11 Manager instances.

- **asngwmgm**
  Clears the statistics for all ASN GW Manager instances

- **asnpcmgr**
  Clears the statistics for all ASN PC-LR Manager instances

- **hamgr**
  Clears the statistics for all HA Manager instances.

- **gtpcmgr**
  Clears the statistics for all GTPC Manager instances.

- **12tpmgr**
  Clears the statistics for all L2TP Manager instances.

- **imsimgr**
  Clears the statistics for all IMSI Manager instances.

**Usage**

Use this command to statistics for all instances of the specified manager.

**Important:** When this command is issued in any context other than the local context, only instances of the specified manager for the current context have the statistics cleared. When the current context is the local context, all instances of the specified manager type in all contexts have the statistics cleared.

**Example**
Clear the statistics for all instances of the A11 manger, by entering the following command:

```
clear congestion-control statistics allmgr
```
clear content-filtering category statistics

This command clears the Category-based Content Filtering application statistics.

Product
CF

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear content-filtering category statistics [ facility srdbmgr instance:<instance_value>]
```

```
facility srdbmgr instance:<instance_value>
```
Cleans logged events for the specified SRDB Manager instance.

- `instance_value` must be an integer from 1 through 8.
- In StarOS 9.0 and later, `instance_value` must be an integer from 1 through 10000.

Usage
Use this command to clear all Category-based Content Filtering application statistics, or statistics for a specific SRDB Manager instance.

Example
The following command clears all Category-based Content Filtering application statistics:

```
clear content-filtering category statistics
```
clear crash

The clear crash command removes a specific crash file or all crash files.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear crash [ list | number crash_num ]
```

<table>
<thead>
<tr>
<th>list</th>
<th>number crash_num</th>
</tr>
</thead>
<tbody>
<tr>
<td>list: removes all crash files.</td>
<td></td>
</tr>
<tr>
<td>number crash_num removes only the crash file specified as crash_num which must be within the range of 1 through 30.</td>
<td></td>
</tr>
</tbody>
</table>

Usage

CLeft crashes for general maintenance activities in cleaning out old, unused, or files which are of no importance.

Example

The following will remove all crash files.

```
clear crash list
```

The following command will remove only crash file 27.

```
clear crash number 27
```
clear credit-control statistics

This command is used to clear credit control statistics.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear credit-control statistics cc-service cc_service_name
```

```
cc-service cc_service_name
Specifies the credit control service name.
cc_service_name must be an existing Credit Control service, and must be an alpha and/or numeric string of 1 through 63 characters in length.
```

Usage
Use this command to clear active credit control statistics.

Example
The following command clears the configured credit control statistics for a service named service1:

```
clear credit-control statistics cc-service service1
```
clear crypto

The clear crypto command clears crypto associations or crypto statistics.

Product

PDSN, HA, GGSN, PDG/TTG, PDIF, SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear crypto { isakmp [ tag map_name | peer peer_ip ] | security-association { counters tag map_name [ tx | rx ] | tag map_name | peer peer_ip } | statistics { ikev2 | ipsec-3gpp-cscf } [ service-ip-address ip-address | service-name name ] }
```

- **isakmp [ tag map_name | peer peer_ip ]**
  - When no keywords are specified, this command clears all of the ISAKMP security associations for the current context.
  - **tag map_name**: Clears the ISAKMP SAs for the specified crypto map. `map_name` is the name of an existing crypto map.
  - **peer peer_ip**: Deletes the ISAKMP SAs for the specified peer. `peer_ip` must be entered in standard IPv4 notation.

- **security-association { counters tag map_name [ tx | rx ] | tag map_name | peer peer_ip }**
  - **counters tag map_name [ tx | rx ]**: Resets the counters for the specified crypto map. `map_name` is the name of an existing crypto map. `tx` specifies that only the transmit SA counters are reset. `rx` specifies that only the receive SA counters are reset. If neither `tx` or `rx` are specified, both transmit and receive SA counters are reset.
  - **tag map_name**: Tears down a Security Association (SA) for the specified crypto map. `map_name` is the name of an existing crypto map.
  - **peer peer_ip**: Clears the SAs for all tunnels who have the peer at the specified IP address. `peer_ip` must be entered in standard IPv4 notation.

⚠️ **Caution**: Modification(s) to an existing crypto map and/or ISAKMP policy configuration will not take effect until the related security association has been cleared.

- **statistics { ikev2 | ipsec-3gpp-cscf } [ service-ip-address ip-address | service-name name ]**
  - **ikev2**: Clears global IKEv2 statistics for the current context.
  - **ipsec-3gpp-cscf**: Clears global CSCF IPSec statistics for the current context.
  - **service-ip-address ip-address**: Clears statistics for the specified service-ip address. `service-name name`: Clears statistics for the specified service name.

Usage

Clear SAs and apply changes to the crypto map or clear the crypto statistics for this context.
Example
The following clears all IKEv2 crypto statistics for the current context:

    clear crypto statistics ikev2
clear cscf service

Resets statistics counters for a specific CSCF service, all CSCF services, or for all services within a specified context (VPN).

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Syntax

clear cscf service

Syntax: clear cscf service { diameter { location-info | policy-control } statistics [ service-name service_name | vpn-name name ] | li-packet-cable statistics [ service-name service_name ] | performance-counters name service_name | statistics name service_name { all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp | vpn-name name } }

diameter { location-info | policy-control } statistics [ service-name service_name | vpn-name name ]
Clears Diameter (DPECA) statistics on the CSCF Rx interface with the configuration information.
service-name service_name: Specifies the name of a CSCF service for which the statistics will be reset.
vpn-name name: Must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

li-packet-cable statistics [ service-name service_name ]
Clears Lawful Intercept statistics.
service-name service_name: Clears Lawful Intercept statistics for a specific CSCF service configured on this system. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

performance-counters name service_name
Clears all CSCF performance counters for a specific CSCF service configured on this system.
name service_name: Must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

statistics name service_name { all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp | vpn-name name }
Clears service statistics for a specific CSCF service configured on this system. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.
all: Clears all CSCF service statistics.
calls: Clears statistics related to CSCF calls.
ip-security: Clears statistics related to CSCF IPSec.
message: Clears statistics for the SIP method MESSAGE.
package-name: Clears statistics for the associated event package.
clear cscf service

- presence: Clears statistics for the “presence” event package.
- reg: Clears statistics for the “reg” event package.
- winfo: Clears statistics for the “watcher-info” event package.
- registrations: Clears statistics related to CSCF registrations, re-registrations, and de-registrations.
- sigcomp: Clears statistics related to CSCF sigcomp.
- tcp: Displays session statistics related to CSCF TCP.
- vpn-name name: Clears statistics for a specific CSCF service configured in a specific context on this system. name must be an existing context and be from 1 to 79 alpha and/or numeric characters.

**Important:** This keyword must be followed by another statistics-related keyword.

**Usage**

Use this command to reset statistics counters for CSCF services. This command will reset the counters in the output of the `show cscf service statistics` command.

**Important:** This command will not clear current registered users and current CSCF sessions.

**Example**

The following command resets all statistics for a service named `cscf1`:

```
clear cscf service statistics name cscf1 all
```
clear cscf sessions

Clears statistics for CSCF sessions on this system.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear cscf sessions { counters { calls | subscription } service service_name | service service_name { all | aor aor | session-id id } }
```

**counters { calls | subscription } service service_name**
Clears counters for all CSCF sessions matching the filter criteria.
calls: Counters associated with calls in CSCF service.
subscription: Counters associated with subscriptions in CSCF service.

**service service_name { all | aor aor | session-id id }**
Clears session information for all CSCF sessions matching the filter criteria.
service service_name: Session statistics on specific CSCF service. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

- **all**: Specifies that session statistics are to be cleared for all sessions on this service.
- **aor aor**: Specifies that session statistics are to be cleared for sessions at this specific AoR. aor must be an existing AoR and be from 1 to 79 alpha and/or numeric characters.
- **session-id id**: Specifies that session statistics are to be cleared for sessions with this ID. id must be an existing session ID and be from 1 to 63 alpha and/or numeric characters.

Usage
Use this command to clear session information for CSCF sessions.

Example
The following command resets all session statistics for a service named cscf1:

```
clear cscf sessions service cscf1 all
```
clear cscf sip

Resets SIP statistics counters for a specific CSCF service, all CSCF services, or for all services within a specified context (VPN) or interface.

**Product**

SCM

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
clear cscf sip statistics [ name service_name [ interface { domain_name domain_name | ip address ip_address } | vpn-name name ]
```

- **name service_name**
  Specifies the name of a CSCF service for which the SIP statistics will be reset. `service_name` must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

- **interface { domain_name domain_name | ip address ip_address }**
  SIP statistics will be reset in this interface.
  - domain name `domain_name`: Specifies the domain associated with the CSCF service. `domain_name` must be an existing domain and be from 1 to 64 alpha and/or numeric characters.
  - ip address `ip_address`: Specifies the destination or source ip address associated with the CSCF service.

- **vpn-name name**
  Specifies the name of a context in which all SIP statistics for all services will be reset. `name` must be an existing context and be from 1 to 79 alpha and/or numeric characters.

**Usage**

Use this command to reset SIP counters found in the output of the `show cscf sip` command.

**Example**

The following command resets the SIP statistics for a service named `cscf1`:

```
clear cscf sip statistics name cscf1
```
clear cscf subscription

Clears all subscriptions for a named service or for individual subscribers within the service.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear cscf subscription service service_name { all | from-aor subscriber_aor to-aor resource_aor }
```

```

service service_name
Specifies the name of a CSCF service for which the subscription(s) will be cleared. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

all | from-aor subscriber_aor to-aor resource_aor
all: Removes all CSCF subscriptions for the specified service.
from-aor subscriber_aor: Removes all CSCF subscriptions for a specified subscriber in a specified service.
subscribed-to resource_aor: Removes all CSCF subscriptions for a specified subscriber in a specified service with a specified subscribed-to resource AoR.

Usage
Use this command to clear subscriptions to enforce policies. This command initiates a SUBSCRIBE request with Expires as 0 in the corresponding subscription dialog.

Example
The following command clear all subscriptions for a CSCF service named cscf1:

```
clear cscf subscription service cscf1 all
```
clear diameter aaa-statistics

This command clears Diameter AAA statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear diameter aaa-statistics [ all | [ group aaa_group ] server diameter_server ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>all</th>
</tr>
</thead>
</table>
| Clears all Diameter server statistics.

<table>
<thead>
<tr>
<th>group aaa_group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears Diameter server statistics for the specified AAA group.</td>
</tr>
<tr>
<td><code>aaa_group</code> must be the name of a AAA group, and must be a string of 1 through 64 characters in length.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>server diameter_server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears Diameter server statistics for the specified Diameter server.</td>
</tr>
<tr>
<td><code>diameter_server</code> must be the name of a Diameter server, and must be a string of 1 through 64 characters in length.</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more } |
|-----------------------------|
| Indicates the output of the command is to be piped (sent) to the command specified. |
| A command to send output to must be specified. |
| For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference. |

Usage

Use this command to clear Diameter AAA statistics.

Example

The following command clears Diameter server statistics for the specified AAA group:

```
clear diameter aaa-statistics group <aaa_group>
```
clear diameter statistics

This command clears Diameter statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

clear diameter statistics [ [ proxy ] endpoint endpoint_name [ peer-host host_id [ peer-realm realm_id ] ] ] [ | { grep grep_options | more } ]

endpoint endpoint_name
Clears endpoint related statistics.
endpoint_name must be the name of an endpoint, and must be a string of 1 through 63 characters in length.

proxy
Clears proxy related statistics.

peer-host host_id
Clears statistics for the specified Diameter peer host ID.
host_id must be the Diameter peer host ID, and must be a string 1 through 255 characters in length.

peer-realm realm_id
Clears statistics for the specified Diameter peer realm.
realm_id must be the Diameter peer realm ID, and must be a string 1 through 127 characters in length.

| { grep grep_options | more }
Indicates the output of the command is to be piped (sent) to the command specified.
A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to clear Diameter statistics.

Example
The following command clears all Diameter statistics for the specified endpoint:

clear diameter statistics endpoint <endpoint_name>
clear dhcp statistics

Deletes all previously gathered statistics for either a specific DHCP server or all DHCP servers configured within the given context.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear dhcp statistics [ dhcp-service svc_name | server ip_address]
```

```
dhcp-service svc_name
```

The name of a specific DHCP service for which to clear statistics. **svc_name** is the name of the DHCP service and can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.

```
server ip_address
```

Specifies the IP address of a specific DHCP server configured in the context for which to clear statistics. **ip_address** must be entered in dotted decimal notation.

Usage
Statistics for a single server can be cleared using the **server** keyword. Statistics for all DHCP servers in the context can be deleted by entering the command with no keywords. This command can be executed from any context configured on the system. If this command is executed from within the local context with no keywords, statistics will be cleared for every DHCP server configured on the system regardless of context. In addition, if the server keyword is used when executing from within the local context, statistics for all DHCP servers configured with the specified name will be cleared regardless of context.

Example
The following command clears statistics for all configured DHCP servers within the context:

```
clear dhcp statistics
```
clear dns-client

Clears DNS cache and/or statistics for a specified DNS client.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear dns-client name { cache [ query-name name | query-type { A | SRV } ] | statistics }
```

dns-client name
Defines the name of the DNS client whose cache and/or statistics are being cleared. `name` must be an existing DNS client and be from 1 to 255 alpha and/or numeric characters in length.

```
cache [ query-name name | query-type { A | SRV } ]
```
Specifies that the cache for the defined DNS client is to be cleared.
query-name `name`: Filters DNS results based on the domain name. `name` must be from 1 to 255 characters in length. `name` is the domain name used to perform the DNS query. `name` is different from the actual domain name which is resolved. For example, to resolve the SIP server for `service.com`, the query name is `_sip._udp.service.com` and the query type is `SRV`.
query-type:
• `A`: Filters DNS results based on domain IP address records (A records).
• `SRV`: Filters DNS results based on service host records (SRV records).

```
statistics
```
Specifies that statistics for the defined DNS client are to be cleared.

Usage
Use this command to clear DNS cache and/or statistics for a specified DNS client.

Example
The following command clears statistics for a DNS client named `domain1.com`

```
clear dns-client domain1.com statistics
```
clear egtpc

Clears enhanced GPRS Tunneling Protocol control plane statistics and counters found in show command outputs and bulk statistics associated with all eGTP-C-related services or those defined by the parameters in this command.

Product
MME, P-GW, S-GW

Privilege
Operator

Syntax

```
clear egtpc statistics [ egtp-service name | interface-type { interface-mme | interface-pgw-ingress | interface-sgw-egress | interface-sgw-ingress } | mme-address ip_address | pgw-address ip_address | sgw-address ip_address ]
```

<table>
<thead>
<tr>
<th>egtp-service name</th>
</tr>
</thead>
</table>
| Clears all statistics and counters associated with a specific eGTP service name. *name* must be an existing eGTP service name and be from 1 to 63 alpha and/or numeric characters.

| interface-type { interface-mme | interface-pgw-ingress | interface-sgw-egress | interface-sgw-ingress } |
|---------------------------|
| interface-mme: Clears statistics and counters derived from all MME interface types associated with this system.
| interface-pgw-ingress: Clears statistics and counters derived from all P-GW ingress interface types associated with this system.
| interface-sgw-egress: Clears statistics and counters derived from all S-GW egress interface types associated with this system.
| interface-sgw-ingress: Clears statistics and counters derived from all S-GW ingress interface types associated with this system.

<table>
<thead>
<tr>
<th>mme-address ip_address</th>
</tr>
</thead>
</table>
| Clears all statistics and counters derived from a specific MME IP address. *ip_address* must be an existing MME IP address and be specified in dotted decimal notation (for IPv4) or colon-separated notation (for IPv6).

<table>
<thead>
<tr>
<th>pgw-address ip_address</th>
</tr>
</thead>
</table>
| Clears all statistics and counters derived from a specific P-GW IP address. *ip_address* must be an existing P-GW IP address and be specified in dotted decimal notation (for IPv4) or colon-separated notation (for IPv6).

<table>
<thead>
<tr>
<th>sgw-address ip_address</th>
</tr>
</thead>
</table>
| Clears all statistics and counters derived from a specific S-GW IP address. *ip_address* must be an existing S-GW IP address and be specified in dotted decimal notation (for IPv4) or colon-separated notation (for IPv6).
**Usage**

Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all eGTP-C-related services or for specific interfaces, services, or IP addresses as specified by parameters in this command.

**Example**

The following command clears eGTP-C statistics and counter associated with all P-GW ingress interfaces configured on this system:

```
clear egtpc statistics interface-type interface-pgw-ingress
```

The following command clears eGTP-C statistics and counter associated with all MME interfaces configured on this system:

```
clear egtpc statistics interface-type interface-mme
```
clear firewall flows

This command is obsolete.
clear firewall ruledef

This command is obsolete.
clear firewall statistics

This command is obsolete.
clear gmm-sm statistics

Deletes all previously gathered GMM-SM statistics within the given context based on the specified criteria.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear gmm-sm statistics [ gmm-only | sm-only ] [ gprs-service srvc_name [ nsei
nsei_id | routing-area mcc mcc_id mnc mnc_id lac lac_id rac rac_id ] ] | [ sgsn-
service srvc_name [ rnc mcc mcc_id mnc mnc_id rnc-id rnc_id | routing area mcc
mcc_id mnc mnc_id lac lac_id rac rac_id ] ]
```

**gmm-only**
Enter this keyword to display only GPRS mobility management (GMM) information for other specified keyword parameters for the current context.

**sm-only**
Enter this keyword to display only session management (SM) information for other specified keyword parameters for the current context.

**gprs-service srvc_name**
Enter this keyword to display the statistics for the specified GPRS service. The display request can be narrowed by adding additional keywords. 

*srvc_name* must be an alphanumeric string of 1 to 63 alphanumeric characters.

**nsei**
Enter this keyword to display the GMM/SM session statistics for the identified network service entity (NSEI).

**sgsn-service srvc_name**
Enter this keyword to display the statistics for the specified SGSN service. The display request can be narrowed by adding additional keywords. 

*srvc_name* must be an alphanumeric string of 1 to 63 alphanumeric characters.

**rnc**
Enter this keyword to fine-tune the display of the GMM/SM session statistics just for the specified (rnc-id) radio network controller (RNC).

**rnc-id rnc_id**
Enter this keyword to identify the specific RNC.

*rnc_id* must be an integer from 0 through 4095.
clear gmm-sm statistics

**Routing Area Commands (A-C)**

Clear GMM/SM statistics

```
Routing-area mcc mcc_id mnc mnc_id lac lac_id rac rac_id
```

Enter the `routing-area` keyword to fine-tune the display of the GMM/SM session statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

**MCC mcc_id**

Enter this keyword to specify the mobile country code (MCC) as part of the identification of the RNC or RA. `mcc_id` must be an integer from 100 through 999.

**MNC mnc_id**

Enter this keyword to specify the mobile network code (MNC) as part of the identification of the RNC or RA. `mnc_id` must be an integer from 00 through 999.

**LAC lac_id**

Enter this keyword to specify the location area code (LAC) as part of the identification of the RNC or RA. `lac_id` must be an integer from 1 through 65535.

**RAC rac_id**

Enter this keyword to specify the routing area code (RAC) as part of the identification of the RNC or RA. `rac_id` must be an integer from 1 through 255.

**Usage**

Use this command to delete statistics for the GMM/SM session configurations for SGSN services.

**Example**

The following command deletes GMM/SM statistics for a specific routing area defined for the GPRS service:

```
clear gmm-sm statistics gprs-service gprs1 routing-area mcc 123 mnc 131 lac 24 rac 11
```

The following command clears all collected information for GMM/SM statistics:

```
clear gmm-sm statistics verbose
```
clear gtpc statistics

Deletes all previously gathered GTPC (GTPv0, GTPv1-C, GTPv1-U) statistics within the given context based on the specified criteria.

**Product**  
GGSN

**Privilege**  
Security Administrator, Administrator, Operator

**Syntax**  

```
clear gtpc statistics [ apn apn_name] [ custom1 ] [ ggsn-service ggsn_name] [ sgsn-address sgsn_address]
```

**apn apn_name**  
Specifies the name of an APN configured in the context for which to delete GTPC statistics.  
`apn_name` can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**custom1**  
Clears the statistics of GTP-C messages for preservation mode and free of charge service.  
This keyword is customer-specific license enabled and used for Preservation-Mode and Free-of-Charge Service which are enabled under customer-specific license. For more information on this support, contact your local representative.

**ggsn-service ggsn_name**  
Specifies the name of a GGSN service configured in the context for which to delete GTPC statistics.  
`ggsn_name` can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**sgsn-address sgsn_address**  
Specifies the IP address of an SGSN for which to delete GTPC statistics.  
`sgsn_address` must be expressed in dotted decimal notation.

**Usage**  
GT-C statistics can be cleared for a single APN, GGSN service, or SGSN. All GTPC statistics in the context can be deleted by entering the command with no keywords.  
This command can be executed from any context configured on the system.  
If this command is executed from within the local context with no keywords, all GTPC statistics will be cleared regardless of context.  
GTPP statistics are not affected by this command.

**Example**  
The following command clears all GTPC statistics within the context:

```
clear gtpc statistics
```
clear gtpc statistics
clear gtppp statistics

Deletes all previously gathered GTPP statistics within the given context based for either single or all charging gateway functions (CGFs).

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

clear gtppp statistics [ cgf-address ip-address]

cgf-address cgf_address
Deletes statistics for a particular CGF. cgf_address is the IP address of the CGF for which statistics are to be deleted. It must be expressed in dotted decimal notation

Usage
Statistics for a single CGF can be cleared using the cgf-address keyword. Statistics for all CGFs in the context can be deleted by entering the command with no keywords.
This command can be executed from any context configured on the system.
If this command is executed from within the local context with no keywords, statistics will be cleared for every CGF configured on the system regardless of context. In addition, if the cgf-address keyword is used when executing from within the local context, statistics for all CGFs configured with the specified name will be cleared regardless of context.

Example
The following command deletes all GTPP statistics for a CGF with an IP address of 192.168.1.42:

clear gtppp statistics cgf-address 192.168.1.42
clear gtpp storage-server local file statistics

This command clears AAAproxy GTPP group level statistics for CDRs stored on the local SMC hard disk.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

clear gtpp storage-server local file statistics [ group name name ]

Usage
If executed from the local context, this command clears statistics for all GTPP groups configured on the system. If executed from the context within which the storage servers (SMC hard disk) is configured, statistics are deleted for only that context.
clear gtpp storage-server statistics

Clears statistics for configured GTPP storage servers (GSS).

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

`clear gtpp storage-server statistics`

Usage
If executed from the local context, this command clears statistics for all GTPP storage servers configured on the system. If executed from the context within which the servers are configured, statistics are deleted for only those servers.
clear gtpu statistics

Clears enhanced GPRS Tunneling Protocol user plane statistics and counters found in show command outputs and bulk statistics associated with all GTP-U-related services or those defined by the parameters in this command.

Product
P-GW, S-GW

Privilege
Operator

Syntax
clear gtpu statistics [ gtpu-service name | peer-address ip_address ]

gtpu-service name
Clears all statistics and counters associated with a specific GTP-U service name. name must be an existing GTP-U service name and be from 1 to 63 alpha and/or numeric characters.

peer-address ip_address
Clears all statistics and counters derived from a specific peer IP address. ip_address must be an existing peer IPv4 or IPv6 address and be specified in dotted decimal notation (for IPv4) or colon-separated notation (for IPv6).

Usage
Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all GTP-U-related services or for specific services or IP addresses as specified by parameters in this command.

Example
The following command clears GTP-U statistics and counter associated with a GTP-U service name gtpu-12 configured on this system:

```
clear gtpu statistics gtpu-service gtpu-12
```
clear hd-storage-policy

Clears statistic information for HD storage policies configured on the system.

Product
HSGW, P-GW, S-GW

Privilege
Operator

Syntax

```
clear hd-storage-policy statistics { all | name name }
```

```
statistics { all | name name }
```

- **all**: Specifies that ACR statistic information for all HD storage policies configured on the system is to be cleared.
- **name name**: Specifies that ACR statistic information for an HD storage policy with the specified name is to be cleared.

Usage
Use this command to clear statistics for HD storage policies configured on the system.

Example
The following command clears statistics for an HD storage policy named `pgwsgw`:

```
clear hd-storage-policy statistics name pgwsgw
```
clear hsgw-service

Clears statistic information for HSGW services configured on the system.

**Product**

HSGW

**Privilege**

Operator

**Syntax**

```
clear hsgw-service statistics { all | name name }
```

- **statistics { all | name name }**
  - **all**: Specifies that HSGW service statistic information for all HSGW services configured on the system is to be cleared.
  - **name name**: Specifies that HSGW service statistic information for an HSGW service with the specified name is to be cleared.

**Usage**

Use this command to clear statistics for HSGW services configured on the system.

**Example**

The following command clears statistics for an HSGW service named `hsgw3`:

```
clear hsgw-service statistics name hsgw3
```
clear ims-authorization

This command clears statistics for all or for a specified IMS Authorization Service.

Product
GGSN, SCM

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear ims-authorization { policy-control statistics [ ims-auth-service service_name ] | service statistics [ name service_name ] } [ | { grep grep_options | more } ]
```

- **ims-auth-service service_name**
  
  Clears statistics for the specified IMSA service. *service_name* must be the name of an IMSA service, and must be a string of 1 through 64 characters in length.

- **grep grep_options | more**
  
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  
  For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to clear IMSA Service statistics.

Example

The following command clears IMSA policy-control statistics for an IMSA service named *test_service*:

```
clear ims-authorization policy-control statistics ims-auth-service test_service
```
clear ip access-group statistics

This command clears all interface ACL statistics and the context level ACL statistics that have been configured in the current context. Be aware that updating an access list also causes all ip access-groups utilizing the list to be cleared.

**Product**

PDSN, GGSN, ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
clear ip access-group statistics
```

**Usage**

Use this command to clear all interface ACL statistics and the context level ACL statistics that have been configured in the current context.

The following command clears the ACL statistics:

```
clear ip access-group statistics
```
clear ip arp

Clears the address resolution protocol cache for a given IP address.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
clear ip arp ip_address
```

Specifies the IP address for which to clear the ARP cache. `ip_address` must be specified using the standard IPv4 dotted decimal notation.

Usage
Clear the ARP cache when network changes have occurred for the case where the cached data may cause undue overhead in routing of packets.

Example
The following command clears the ARP cache for the IP address 1.2.3.4:

```
clear ip arp 1.2.3.4
```
clear ip bgp peer

Resets BGP connections for all peers or for specified peers in the current context.

Product
HA

Privilege
Security Administrator, Administrator

Syntax
```
clear ip bgp peer {ip_address| all | as as_num} [in | out | soft | vpnv4 ]
```

**ip_address**
The IP address of the neighbor for which BGP connections should be reset. *ip_address* is an IPv4 address in dotted-decimal notation.

**all**
Reset BGP connections for all peers.

**as as_num**
Reset BGP connections for all peers in the specified AS. *as_num* must be an integer from 1 through 65535.

**in**
Soft reconfigure inbound updates.

**out**
Soft reconfigure outbound updates.

**soft**
Soft reconfigure inbound and outbound updates.

**vpnv4**
Clears bgp sessions with the vpnv4 address family.

Usage
Use this command to BGP information for the current context.

Example
The following command resets BGP connections for all neighbors:
```
clear ip bgp peer all
```
clear ip localhosts

This command removes the host specified from the current context’s local host list for IP address mappings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
clear ip localhosts [ host_name ]
```

*host_name*
Specifies the name of the host to be removed. Value must be a string from 1 to 1023 characters. When omitted, all local host name mappings will be removed.

**Usage**
Clear a host name when it is no longer valid for the current context to access. The host name specified will be unrecognized by the current context once the command is performed.

**Example**

```plaintext
clear ip localhosts
clear ip localhosts 1.2.3.4
clear ip localhosts remoteABC
```
clear ip ospf process

Clears OSPF database information for the current context and re-establishes neighbor adjacency.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
clear ip ospf process
```

**Usage**
Use this command to clear the OSPF database information for the current context and re-establishes neighbor adjacency.

**Example**
The following command clears the OSPF database information for the current context and re-establishes neighbor adjacency:

```
clear ip ospf process
```
clear ipv6 neighbors

Clears an ipv6 address from the neighbor cache.

**Product**
PDIF

**Privilege**
Administrator, Security Administrator

**Syntax**

```
clear ipv6 neighbors ipaddress
```

**Usage**
Clears a specific address from the neighbor cache.

**Example**

Use the following example to clear 3ffe:ffff:101::230:6eff:fe04:d9aa/48:

```
```
clear l2tp

Clears all or specific L2TP statistics or clears and disconnects all or specified sessions or tunnels.

Product
PDSN, GGSN, LNS

Privilege
Security Administrator, Administrator, Operator

Syntax

```
statistics [ lac-service service_name | lns-service service_name | peer-address ip_address ]
```

With no optional keywords specified, this command clears all L2TP statistics for the current context.

- **lac-service service_name**: Clears all L2TP statistics for the specified LAC service in the current context.
- **lns-service service_name**: Clears all L2TP statistics for the specified LNS service in the current context.
- **peer-address ip_address**: Clears all L2TP statistics for the destination (peer LNS) at the specified IP address. The IP address is specified using the standard IPv4 dotted decimal notation.

```
tunnels { all [ clear-sa ] | callid call_id | lac-service service_name [ clear-sa ] | peer-address ip_address [ clear-sa ] }
```

- **all**: Clears all tunnels in the current context.
- **lac-service service_name**: Clears all tunnels in the current context that belong to the specified LAC service and closes the tunnels.
- **lns-service service_name**: Clears all tunnels in the current context that belong to the specified LNS service and closes the tunnels.
- **peer-address ip_address**: Clears all tunnels in the current context whose destination (peer LNS) is the system at the specified IP address. The IP address is specified using the standard IPv4 dotted decimal notation.
- **callid call_id**: Uses the unique identifier that specifies a particular tunnel in the system to clear that tunnel and disconnect it. The output of the command `show l2tp tunnels` contains a field labeled Callid Hint which lists the call id information to use with this command. This is an 8-Byte Hexadecimal number.
- **clear-sa**: If any security associations have been established they are cleared.

Usage
Clear L2TP all or specific L2TP statistics or clear sessions in a tunnel and disconnect the tunnel.

Example
To clear all L2TP statistics for the current context, use the following command:
```
clear l2tp statistics
```

To clear all L2TP statistics for the LAC service named lac1, use the following command:
```
clear l2tp statistics lac-service lac1
```
Use the following command to clear L2TP statistics for the LNS peer at the IP address 10.10.10.100:

```
clear l2tp statistics peer-address 10.10.10.100
```

The following command clears and closes all tunnels in the current context:

```
clear l2tp tunnels all
```

The following command clears and closes all tunnels for the LAC service named lac2:

```
clear l2tp tunnels lac-service lac2
```

The following command clears and closes all tunnels the peer at the IP address 10.10.10.110:

```
clear l2tp tunnels peer-address 10.10.10.110
```
clear lawful-intercept

Clears information pertaining to lawful interception capability.

**Product**
PDSN, HA, LNS, GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
clear lawful-intercept statistics
```

**Usage**
Use this command to clear statistics pertaining to Lawful Intercept functionality.

**Important:** You must log in to the system through a Secure Shell (SSH) using a system account that has administrator privileges to use this command. For details on using the Lawful Intercept capability of the system, refer to System Administration and Configuration Guide.

**Example**
The following clears all statistics for the Lawful Intercept functionality.

```
clear lawful-intercept statistics
```
clear lma-service statistics

Clears Local Mobility Anchor statistics and counters found in show command outputs and bulk statistics associated with all LMA services or a specific service defined by the parameter in this command.

**Product**
P-GW

**Privilege**
Operator

**Syntax**

```
clear lma-service statistics [ name servie_name ]
```

- **name servie_name**
  Clears statistics and counters for a specific LMA service name. `name` must be an existing LMA service name and be from 1 to 63 alpha and/or numeric characters.

**Usage**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all LMA services or for a specific LMA service.

**Example**

The following command clears statistics and counters for an LMA service named `lma3`:

```
clear lma-service statistics name lma3
```
clear local-user

Clears information pertaining to local-user administrative accounts.

Product

All

Privilege

Security Administrator

Syntax

```
clear local-user { database [ -noconfirm ] | statistics | username name lockout }
```

**database [ -noconfirm ]**

Clears the local-user database. This command deletes all information for all local-user accounts.

⚠️ **Caution:** Use this command only in the event of security concerns or to address concerns of the local-user account database integrity.

**statistics**

Clears statistics pertaining to local-user accounts.

**username name lockout**

Removes lockouts associated with specific local-user accounts.

*name* is the name of the local-user account and can consist of from 3 to 16 alpha and/or numeric characters and is case sensitive.

Usage

This command can be used to remove local-user account lockouts, reset local-user-related statistics to 0, or to delete the local-user database.

Example

The following command removes the lockout placed on a local-user account named *SecureAdmin*.

```
clear local-user username SecureAdmin lockout
```
clear mag-service statistics

Clears Mobile Access Gateway statistics and counters found in show command outputs and bulk statistics associated with all MAG services or a specific service defined by the parameter in this command.

Product
HSGW, S-GW

Privilege
Operator

Syntax

```plaintext
clear mag-service statistics [ name servie_name ]
```

**name servie_name**
Clears statistics and counters for a specific MAG service name. *name* must be an existing MAG service name and be from 1 to 63 alpha and/or numeric characters.

Usage
Use this command to clears statistics and counters in show command outputs and bulk statistics for all MAG services or for a specific MAG service.

Example
The following command clears statistics and counters for a MAG service named *mag1*

```plaintext
clear mag-service statistics name mag1
```
clear maximum-temperatures

Clears information pertaining to component maximum temperatures.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

clear maximum-temperatures

Usage
Reset the timestamp to the current time and clear previous maximum temperatures for all temperature monitored components. This may be useful when preparing to study system performance, monitor usage, or trouble shoot the administrative interfaces.

Example
The following command resets the maximum temperature statistics for all monitored chassis components.

clear maximum-temperatures
clear mipfa statistics

This command clears the statistics for the mobile IP foreign agent. The statistics for a specific foreign agent service may be cleared by explicit command.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator

Syntax

clear mipfa statistics [ fa-service name | peer-address ip_address ]

fa-service name | peer-address ip_address

fa-service name: Indicates the statistics for a specific service are to be cleared where the service is as specified by name. “Total sessions” counters for all peers associated with the service are also reset. name must be an existing FA service name.

peer-address ip_address: Indicates the statistics for the specific IP address, ip_address, are to be cleared. “Total sessions” counter for the specified peer is also reset. The IP address is specified using the standard IPv4 dotted decimal notation.

Usage
Clear all statistics for the MIP foreign agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

Example
The following clears all statistics for the mobile IP foreign agent.

    clear mipfa statistics

The following command clears the statistics for the example service only.

    clear mipfa statistics fa-service sampleService peer-address 1.2.3.4
clear mipha statistics

This command clears the statistics for the mobile IP home agent. The statistics for a home agent service may be cleared by explicit command.

**Product**
HA

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear mipha statistics [ ha-service name | peer-address ip_address ]
```

- **ha-service name | peer-address ip_address**
  - indicates the statistics for a specific service are to be cleared where the service is specified by name. “Total sessions” counters for all peers associated with the service are also reset. name must be an existing HA service name.
  - indicates the statistics for the specific IP address, are to be cleared. “Total sessions” counter for the specified peer is also reset. The IP address is specified using the standard IPv4 dotted decimal notation.

**Usage**
Clear all statistics for the MIP home agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

**Example**
The following clears all statistics for the mobile IP foreign agent.

```
clear mipha statistics
```

The following command clears the statistics for the example service only.

```
clear mipha statistics ha-service sampleService
```
```
clear mipha statistics peer-address 1.2.3.4
```
clear mme-service db statistics

This command clears the MME database statistics for MME sessions for all or specific session instances on this system.

**Product**
MME

**Privilege**
Inspector

**Syntax**

```
clear mme-service db statistics [instance smgr_instance]
```

*instance smgr_instance*

This keyword specifies that MME database statistics are to be removed for a specific instance of session manager running for MME service. *smgr_instance* must be specified as an instance ID in the range 0 through 4294967295. If instance is not specified database statistics of all instances will be removed.

**Usage**

Use this command to clear/remove database statistics for all or a particular instance of session manager for MME services on this system.

**Example**

The following command removes/clears the database statistics of all instances of the MME service on a system:

```
clear mme-service db statistics
```

clear mme-service db record

This command clears the MME database records all instances of session manager running for MME service filtered with IMSI or GUTI as criteria.

**Product**
MME

**Privilege**
Inspector

**Syntax**

```
clear mme-service db record {imsi imsi_identifier | callid call_id | guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value} [ | { grep grep_options | more } ]
```

**imsi imsi_identifier**
This keyword specifies the filter criteria as International Mobile Subscriber Identity (IMSI)
`imsi_identifier` to clear the database records of a session instance.
`imsi_identifier` is a 15 character IMSI field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘‘). For example; ‘$’.

**callid call_id**
This keyword specifies the filter criteria as call id `call_id` to clear the database records of a session instance.
`call_id` must be specified as an 8-byte hexadecimal number.

**guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value**
This set of keyword specifies the filter criteria as Globally Unique Temporary Identifier (GUTI) to clear the database records for MME service.
The GUTI is constructed from the GUMMEI and the M-TMSI where GUMMEI is constructed from PLMN (MMC and MNC) `plmn_id` and MME Identifier is constructed from an MME Group ID (MMEGI) `mme_grp_id` and an MME Code (MMEC) `mme_code`.
Within the MME, the mobile is identified by the M-TMSI `mtmsi_value`.

**Usage**
Use this command to clear/remove database records for all or a particular instance of session manager for MME services on this system with IMSI or GUTI as filter criteria.

**Example**
The following command clears the summary database records of a session instance for subscriber having IMSI as 123455432112345 in the MME service:

```
clear mme-service db record imsi 123455432112345
```
clear mme-service statistics

This command clears the service statistics of an MME service specified by various criteria.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
clear mme-service statistics [emm-only [mme-service mme_svc_name| peer-id peer_identifier]] | esm-only [mme-service mme_svc_name| peer-id peer_identifier] | slap [mme-service mme_svc_name| peer-id peer_identifier] | sctp [mme-service mme_svc_name]
```

- **emm-only**
  This keyword sets the filter criteria as MME service name or peer MME identifier to clear all EPS mobility management (EMM) related statistics.

- **esm-only**
  This keyword sets the filter criteria as MME service name or peer MME identifier to clear all EPS session management (ESM) related statistics.

- **slap**
  This keyword sets the filter criteria as MME service name of peer MME identifier to clear all S1-AP statistics.

- **sctp**
  This keyword sets the filter criteria as MME service name of peer MME identifier to clear all SCTP statistics.

- **mme-service mme_svc_name**
  This keyword sets the filter criteria as MME service name to clear all service statistics.

- **peer-id peer_identifier**
  This keyword sets the filter criteria as identifier of MME peer to clear all service statistics.

Usage

This command is used to clear the statistical information of an MME service based on various filter criteria.

Example

The following command clears the service session statistics of all MME service on a system:

```
clear mme-service statistics
```
clear mme-service statistics
clear mme-service statistics

This command clears the service statistics of an MME service specified by various criteria.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
clear mme-service statistics [emm-only [mme-service mme_svc_name| peer-id peer_identifier]] | esm-only [mme-service mme_svc_name| peer-id peer_identifier] | slap [mme-service mme_svc_name| peer-id peer_identifier] | sctp [mme-service mme_svc_name]
```

- **emm-only**
  This keyword sets the filter criteria as MME service name or peer MME identifier to clear all EPS mobility management (EMM) related statistics.

- **esm-only**
  This keyword sets the filter criteria as MME service name or peer MME identifier to clear all EPS session management (ESM) related statistics.

- **slap**
  This keyword sets the filter criteria as MME service name of peer MME identifier to clear all S1-AP statistics.

- **sctp**
  This keyword sets the filter criteria as MME service name of peer MME identifier to clear all SCTP statistics.

- **mme-service mme_svc_name**
  This keyword sets the filter criteria as MME service name to clear all service statistics.

- **peer-id peer_identifier**
  This keyword sets the filter criteria as identifier of MME peer to clear all service statistics.

**Usage**

This command is used to clear the statistical information of an MME service based on various filter criteria.

**Example**

The following command clears the service session statistics of all MME service on a system:

```
clear mme-service statistics
```
clear mme-service statistics
clear multicast-sessions

Disconnects broadcast-multicast sessions based on specified criteria.

Product
PDSN, GGSN

Privilege
Security Administrator Operator

Syntax

clear multicast-sessions [ -noconfirm ] [ keywords ] [ verbose ]

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

all
Disconnects all multicast sessions.

callid call_id
Clears the call specified by call_id. The call ID must be specified as an 8-digit hexadecimal number.

card-num psc_num
The slot number of the packet processing by which the multicast session is processed. psc_num is a slot number from 1 through 7 or 10 through 16.

flowid id
Clears calls for a specific BCMCS flow, defined by id. The flow ID must be a hexadecimal number.

flowid-type [ flow | program ]
Clears multicast sessions according to the type of flow.
flow: Clears all multicast sessions for the flow ID type "flow".
program: Clears all multicast sessions for the flow ID type "program".

mcast-address ipv4_address
Clears multicast sessions for a specific multicast address. Must be followed by the IP address of an interface, using dotted decimal notation.

pcf ipv4_address
Clears multicast sessions connected via the packet control function defined by ipv4_address. The address must be specified using the standard IPv4 dotted decimal notation.

pdsn_service name
Clears multicast sessions connected to the packet data service name. The packet data service must have been previously configured.
verbose
Indicates the output should provide as much information as possible. If this option is not specified then the output is the standard level which is the concise mode.

Usage
Clear multicast sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be useful when preparing for maintenance activities such that connects may be cleared to perform any necessary procedures.
The keywords are filters that modify or filter the criteria for deciding which sessions to clear and are described below. Multiple keywords can be entered on a command line.
When multiple keywords are specified, the multicast sessions deleted must meet the specifications of all of the keywords.

Example
The following command clears the broadcast-multicast sessions having multicast address 1.2.3.4:

clear multicast-sessions mcast-address 1.2.3.4

The following command clears the broadcast-multicast session(s) having call id 00004e22:

clear multicast-sessions callid 00004e22
clear orbem statistics

Clears the CORBA element manager interface related statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear orbem statistics
```

**Usage**

Clear the statistics to reset them to zero for the object request broker element manager interface. This may be useful when preparing to study system performance, monitor usage, or troubleshoot the administrative interfaces.

**Example**

The following command resets the statistics for the ORB element manager.

```
clear orbem
```
clear pdg-service statistics

Deletes all previously gathered statistics for a specific PDG service or all PDG services configured within a context.

Product
PDG/TTG

Privilege
Security Administrator, Administrator, Operator

Syntax

clear pdg-service statistics [ name service_name ]

name service_name

Specifies the name of a specific PDG service configured in the context for which to clear statistics. service_name is the name of the PDG service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Usage

Usage Statistics for a single PDG service can be cleared using the name keyword. Statistics for all PDG services in the context can be deleted by entering the command with no keywords.

If this command is executed from within the local context with no keywords, statistics will be cleared for every PDG service configured on the system regardless of context. In addition, if the name keyword is used when executing from within the local context, statistics for all PDG services configured with the specified name will be cleared regardless of context.

Example

Example(s) The following command clears statistics for a PDG service named pdg1:

  clear pdg-service statistics pdg1
clear pgw-service

Clears PDN Gateway statistics and counters found in show command outputs and bulk statistics associated with all P-GW services or a specific service defined by the parameter in this command.

Product
P-GW

Privilege
Operator

Syntax

```
clear pgw-service statistics { all | name service_name }
```

- **all**
  Clears statistics and counters for all P-GW services on the system.

- **name service_name**
  Clears statistics and counters for a specific P-GW service name. *name* must be an existing P-GW service name and be from 1 to 63 alpha and/or numeric characters.

Usage
Use this command to clear statistics and counters in show command outputs and bulk statistics for all P-GW services or for a specific P-GW service.

Example
The following command clears statistics and counters for an P-GW service named *pgw5*:

```
clear lma-service statistics name pgw5
```
clear port

Clears port related statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear port { datalink counters { all | slot/port } | npu counters { all | slot/port [ untagged | vlantag_id ] } }
```

datalink

Clear the data link port statistics.

npu

Clear statistics for the network processing unit port.

all

Clear counters for all datalink or NPU ports.

slot/port

Clear the statistics for the specified slot and port number.

untagged

Clear NPU statistics for all ports that do not have a VLAN tag.

vlan tag_id

Clear NPU statistics for the port that has the specified VLAN tag ID. `tag_id` must be a previously configured VLAN tag id.

Usage

Manually clear the statistics for a specified port. This is useful when preparing to trouble shoot or monitor the system.

Example

The following command clears the data link related statistics for port 1 in slot 17.

```
clear port datalink counters 17/1
```

The following command clears the network processing unit related statistics for port 1 in slot 17.

```
clear port npu counters 17/1
```
clear port
clear ppp statistics

Clears point-to-point protocol related statistics. All PPP statistics may be cleared or just those for a specific packet data service may be cleared.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
clear ppp statistics [ggsn-service ggsn_name | lns-service lns_name | pcf-address [pcf_ip_addr | all] | pdsn-service pdsn_name ]
```

- **ggsn-service ggsn_name**
  Display statistics only for the time the session is connected to the specified ggsn_name.

- **lns-service lns_name**
  Display statistics only for the time the session is connected to the specified lns_name.

- **pcf-address [pcf_ip_addr | all]**
  Display statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. pcf_ip_addr must be specified using the standard IPv4 dotted decimal notation.

- **pdns-service pdsn_name**
  Specifies the service as pdsn_name which is to have only its statistics cleared.

**Usage**

Allows you to manually reset PPP statistics when it is desired to have counts begin again from a specific point in time.

**Example**

The following clears the statistics for all PPP counters and services.

```
clear ppp statistics
```

The following clears only the point-to-point protocol statistics for the service named sampleService.

```
clear ppp statistics pdsn-service sampleService
```
clear prepaid 3gpp2 statistics

This command clears all of the statistics counters for 3GPP2 Pre-paid accounting. Statistics may be cleared for all services or for an individual service.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear prepaid 3gpp2 statistics { all | {ggsn-service | ha-service | lns-service | pdsn-service} {all | name service_name} }
```

- **all**
  This keyword clears prepaid statistics for all services.

- **ggsn-service**
  Clear statistics for GGSN service(s).

- **ha-service**
  Clear statistics for HA service(s).

- **lns-service**
  Clear statistics for LNS service(s).

- **pdsn-service**
  Clear statistics for PDSN service(s).

```
{ all | name service_name }
```

- **all**: Clear statistics for all services of the specified type.
- **name service_name**: Clear statistics for the service named *service_name* of the specified service type.

**Usage**

Use this command to clear Pre-paid statistics for a particular named service or for all services.

**Example**

To clear statistics for a PDSN service name PDSN1, enter the following command:

```
clear prepaid 3gpp2 statistics pdsn-service name PDSN1
```
clear prepaid wimax

This command clears all of the statistics counters for WiMAX prepaid accounting. Statistics may be cleared for all services or for an individual service.

Product
ASN GW

Privilege
Operator

Syntax

```
clear prepaid wimax statistics { all | asngw-service { all | nameservice_name } | ha-service { all | nameservice_name } }
```

- **all**
  This keyword clears prepaid statistics for all services.

- **asngw-service**
  Clears prepaid statistics for ASN GW service(s).

- **ha-service**
  Clears prepaid accounting statistics for HA service(s).

```
{ all | name service_name }
```

- **all**: Clears statistics for all services of the specified type.
- **name service_name**: Clears statistics for the service named `service_name` of the specified service type.

Usage

Use this command to clear prepaid WiMAX accounting statistics for named service or for all services.

Example

The following command clears prepaid WiMAX accounting statistics for an ASN GW service name `asn1`:

```
clear prepaid wimax statistics asngw-service name asn1
```
clear qos npu stats

Clears information pertaining to NPU QoS priority queue bandwidth allocation and sharing.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear qos npu stats inter-subscriber traffic slot slot_num
```

```
inter-subscriber traffic slot slot_num
```

Clears inter-subscriber traffic statistics for the application or line card installed in the specified slot. `slot_num` indicates the number of the chassis slot in which the card is installed and can be configured to any integer value from 1 through 48.

Usage
Allows you to manually reset statistics pertaining to NPU QoS priority queue bandwidth allocation.

Example
The following command clears statistics for a card installed in chassis slot 4:

```
clear qos npu stats inter-subscriber traffic slot 4
```
clear radius accounting archive

This command clears archived RADIUS accounting messages associated with a AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed depending on the option chosen. The scope of the command is limited to the context in which it is executed including for local context.

---

**Important:** This command is only available in StarOS 8.3 and later. For more information, please contact your local service representative.

---

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
clear radius accounting archive { all | radius group group_name } [ -noconfirm ]
```

- `all`
  Cuts all archived RADIUS accounting messages in the context.

- `radius group group_name`
  Cuts all archived RADIUS accounting messages for the specified group.
  `group_name` must be the name of a RADIUS group, and must be a string of 0 through 64 characters in length.

- `-noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to clear the archived RADIUS accounting messages associated with a AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed.

**Example**

Use the following command to clear all archived RADIUS accounting messages for the group named `test12`.

```
clear radius accounting archive radius group test12
```
clear radius counters

Clears statistics for RADIUS servers and server group. The statistics for all RADIUS servers or server group may be cleared or only a specified server.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear radius counters { all | radius group group_name| server ip_address [ port number ] }
```

- `all`: Clears statistics for all servers.
- `server ip_address [ port number ]`: Clears statistics only for the server specified by `ip_address`. Optionally specify the port which is to have its RADIUS statistics cleared, where port number must be an integer from 0 through 65535. `ip_address` must be specified using the standard IPv4 dotted decimal notation.
- `radius group group_name`: Clears all configured authentication / accounting servers in the specified RADIUS group. `group_name` must be name of server group configured in specific context for authentication/accounting, and must be a string of 1 through 63 characters in length.

Usage
Clear the statistics to reset them to zero prior to logging or monitoring the system for troubleshooting, performance measurements, etc.

Example
The following command clears the statistics for all RADIUS servers.

```
clear radius counters all
```

The following command resets the statistics only for the server 1.2.3.4.

```
clear radius counters server 1.2.3.4
```

The following command resets the statistics only for the server group named `star1`.

```
clear radius counters radius group star1
```
clear rohc statistics

This command clears statistics and counters collected since the last reload or clear command was issued for ROHC IP header compression.

Product
PDSN

Privilege
Administrator, Config-administrator, Operator, Inspector

Syntax

```
clear rohc statistics [ pdsn-service pdsnsvc_name ]
```

**pdsn-service pdsnsvc_name**
Clear ROHC statistics and counters for the specified PDSN service.

Usage
Use this command to clear ROHC statistics for all services or for a specific PDSN.

Example
The following command clears ROHC statistics and counters for the PDSN service named pdsn1:

```
clear rohc statistics pdsn-service pdsn1
```
clear rp service-option

Clears the R-P interface service option statistics.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator

Syntax

clear rp service-option statistics [ number option_num | psdn-service psdn_name ]

- number option_num | psdn-service psdn_name
  Default: clear the statistics for all service options and all packet data services.
  number option_num specifies the R-P service option number for which the statistics are to be cleared.
  option_num must be a value in the range 0 through 1000.
  psdn-service psdn_name specifies the service as psdn_name which is to have only its statistics cleared.

Usage
Clear the R-P service option statistics prior to monitoring the system for benchmarking or for detecting areas of further research.

Example
The following resets the service option statistics for service option 23 and packet data service sampleService, respectively.

clear rp service-option statistics number 23 clear rp service-option statistics psdn-service sampleService
clear rp statistics

Clears the R-P interface statistics. The statistics for a specific packet data server or peer node may be cleared if specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator

Syntax

clear rp statistics [ pdsn-service name | peer-address [ peer_address | all ] ]


default: clear all R-P associated statistics.

pdns-service name: specifies the packet data service specified by name is to have its statistics reset.

peer-address [ peer_address | all ]: specifies that statistics for the specified peer, or all peers, are to be cleared. ip_address must be specified using the standard IPv4 dotted decimal notation.

Usage
Clear the statistics to prepare for monitoring the system.

Example
The following command resets all the associated statistics for the R-P interfaces.

clear rp statistics

The following clears the statistics for the packet data service sampleService.

clear rp statistics pdsn-service sampleService

The following command resets the statistics associated with peer node with IP address 1.2.3.4.

clear rp statistics peer-address 1.2.3.4
clear session disconnect-reasons

Clears the session disconnect reason statistics for all sessions on the system.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear session disconnect-reasons
```

Usage

Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

Example

```
clear session disconnect-reasons
```
clear session setuptime

Clears the session setup time statistics for PCFs or SGSNs. If no keyword is specified the summary statistics displayed by the `show session setuptime` command are cleared.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clearsessionsetuptime { pcf { pcf_addr | all } | sgsn { sgsn_addr | all } }
```

- **pcf { pcf_addr | all }**
  - `pcf_addr`: Clear the setup time counters for the PCF at the specified IP address. `pcf_addr` must be an IP v4 address expressed in dotted decimal notation.
  - `all`: Clear the setup time counters for all PCFs.

- **sgsn { sgsn_addr | all }**
  - `sgsn_addr`: Clear the setup time counters for the SGSN at the specified IP address. `sgsn_addr` must be an IP v4 address expressed in dotted decimal notation.
  - `all`: Clear the setup time counters for all SGSNs.

**Usage**
Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

**Example**
To clear the statistics for the PCF at IP address 192.168.100.10, enter the following command:

```
clear session setuptime pcf 192.168.100.10
```
clear session subsystem

Clears all session subsystem statistics for the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

clear session subsystem

Usage
Clear the statistics in preparation for a troubleshooting or monitoring session so that the counters are at a well known values.

Example

clear session subsystem
clear sgtpu statistics

Clears all SGTPU statistics for the current context.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```plaintext
clear sgtpu statistics [ ggsn-address ipv4_address | iups-service iups_srvc_name |
| rnc-address ipv4_address | sgtp-service sgtp_srvc_name |gprs-service
|gprs_srvc_name nsei nse_id ]
```

Usage
Clear the statistics in preparation for a troubleshooting or monitoring session so that the counters.

Example

```plaintext
clear sgtpu statistics gprs-service SGSN1Gprs1 nsei 2445
```
clear sgw-service statistics

Clears Serving Gateway statistics and counters found in show command outputs and bulk statistics associated with all S-GW services or a specific service defined by the parameter in this command.

Product
S-GW

Privilege
Operator

Syntax

```
clear sgw-service statistics { all | name service_name }
```

**all**
Clears statistics and counters for all S-GW services configured on the system.

**name service_name**
Clears statistics and counters for a specific S-GW service name. `service_name` must be an existing S-GW service name and be from 1 to 63 alpha and/or numeric characters.

Usage
Use this command to clears statistics and counters in show command outputs and bulk statistics for all S-GW services or for a specific S-GW service.

Example
The following command clears statistics and counters for an S-GW service named `sgw3`:

```
clear sgw-service statistics name sgw3
```
clear snmp trap

Clears all SNMP event trap notifications from the buffer.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear snmp trap { history | statistics }
```

- **history**
  Clears all SNMP historical trap information from system buffer.

- **statistics**
  Clears all SNMP event trap information from system buffer.

Usage

Use this command to empty the buffer of all SNMP trap notifications.

Example

Following command clears the all historical SNMP traps from the system buffer:

```
clear snmp trap history
```
clear srp checkpoint statistics

Clears the SRP checkpoint interface statistics.

**Product**
HA, GGSN PDIF

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
clear srp checkpoint statistics
```

**Usage**
Clears the srp checkpoint statistics to prepare for srp monitoring.

**Example**
The following command resets all the associated statistics for srp checkpoint.

```
clear srp checkpoint statistics
```
clear srp statistics

Clears the SRP statistics.

Product
HA, GGSN PDIF

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear srp statistics
```

Usage
Clears the srp statistics to prepare for srp monitoring.

Example
The following command resets all the associated statistics for srp.

```
clear srp statistics
```
clear subscribers

Dis_connections subscribers based on specified criteria.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
clear subscribers [ keywords ] [ verbose ] [ -noconfirm ]
```

The keywords are filters that modify or filter the criteria for deciding which subscriber sessions to clear and are described below. Multiple keywords can be entered on a command line. When multiple keywords are specified, the subscriber sessions deleted must meet the specifications of all of the keywords.

For example, if you enter the following command:

```
clear subscribers ip-pool pool1 card-num 1
```

Only subscriber sessions that were assigned an IP address from the IP pool named `pool1` and are also being processed by the processing card in slot 1 are cleared. All other subscriber sessions that do not meet these criteria remain and are not cleared.

- `-noconfirm`
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Important**: The Operator privilege does not have access to this keyword.

- `active`
Only disconnects subscribers who currently have active sessions.

- `all`
Dis_connections all subscribers.

**Important**: The Operator privilege does not have access to this keyword.

- `apn name`
Clears all PDP contexts accessing a specific access point name (APN).

`apn_name` is the name of the APN and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- `asn-peer-address ip_address`
Clears information for subscribers on an ASN GW trusted peer.

`ip_address` is the IPv4 address of the ASN GW peer server in dotted decimal notation.
### Exec Mode Commands (A-C)

**clear subscribers**
Clears counters for subscribers accessing the ASN GW service.

**asn-gw-service service_name**
Clears counters for subscribers accessing the ASN GW service.

**asn-pc-service service_name**
Clears counters for subscribers accessing the ASN PC service.

**callid id**
Clears the call specified by call_id. The call ID must be specified as a 4-byte hexadecimal number.

**card-num card_num**
The slot number of the processing card by which the subscriber session is processed. card_num is a slot number from 1 through 7 or 10 through 16.

**ccoa-only**
This option clears the subscribers that registered a MIP co-located COA directly with the HA. This option is only valid when MIP HA session license is enabled.

**configured-idle-timeout [ < | > | greater-than | less-than ] value**
Disconnects subscribers whose idle timeout matches the specified criteria. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.

**connected-time [ < | > | greater-than | less-than ] value**
Disconnects subscribers who have been connected for the specified length of time.

**cscf-service service_name**
Clears all subscribers from the specified CSCF service.

**css-delivery-sequence name**

---

**Important:** This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.
clear subscribers

**css-service** *name*

**Important:** This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

**dhcp-server** *address*
Clears all PDP contexts that currently possess an IP address assigned from a specific DHCP server. *dhcp_address* is the IP address of the DHCP server expressed in dotted decimal notation.

**dormant**
Only disconnect subscriber sessions that are dormant (not transmitting or receiving data).

**fa** *address*
Disconnects all subscribers connected to the foreign agent specified by *fa_address*. The address must be specified using the standard IPv4 dotted decimal notation.

**fa-service** *name*
Disconnects all subscribers connected to the foreign agent specified by *fa_name*. The foreign agent name must have been previously defined.

**firewall** { not-required | required }
Clears all subscriber information for the specified subscribers:
- **not-required:** Subscribers for whom firewall processing is not-required.
- **required:** Subscribers for whom firewall processing is required.

**firewall-policy** *fw_policy_name*
This keyword is obsolete.

**ggsn-service** *name*
Clears all PDP contexts accessing a specific GGSN service.
*ggsn_name* is the name of the APN and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**gsm-traffic-class** { background | conversational | interactive { priority } | streaming }
Subscribers whose traffic matches the specified 3GPP traffic class.
- **background:** 3GPP QoS background class.
- **conversational:** 3GPP QoS conversational class.
- **interactive:** 3GPP QoS interactive class. Must be followed by a traffic priority. priority can be configured to any integer value from 1 to 3.
- **streaming:** 3GPP QoS streaming class.

**gtp-version**
Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1). The following filter keywords are valid with this command:
active-charging-service, apn, asngw-service, asnp-service, asn-peer-address, bearer-establishment, callid, card-num, coaa-only, configured-idle-timeout, connected-time, csclf-service, dhcp-server, fa, fa-service, firewall, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, ha, ha-ipsec-service, ha-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, network-requested, network-type, pcf, pdg-service, pdif-service., pdsn-service, plmn-type, rulebase, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

```ha address```
Disconnects all subscribers connected to the home agent specified by `ha_address`. The address must be specified using the standard IPv4 dotted decimal notation.

```ha-ipsec-only```
Disconnects all MIP HA sessions with IPsec tunnels.

```ha-service name```
Disconnects all subscribers connected to the home agent specified by `ha_name`. The home agent name must have been previously defined.

```hsgw-service name```
Disconnects subscribers using this HRPD Serving Gateway (HSGW) service configured on this system. `name` must be an existing HSGW service and be from 1 to 63 alpha and/or numeric characters.

```idle-time [ < | > | greater-than | less-than ] value```
Disconnects subscribers whose idle time matches the specified length of time.

- `<`: Filters output so that only information less than the specified value is cleared.
- `>`: Filters output so that only information greater than the specified value is cleared.
- `greater-than`: Filters output so that only information greater than the specified value is cleared.
- `less-than`: Filters output so that only information less than the specified value is cleared.

`value`: If no other filtering options are specified only output matching `value` is cleared. If `value` is not specified all data is cleared. `value` must be an integer from 0 through 4294967295.

```ims-auth-service name```
Disconnects subscribers using this IMS Authorization Service configured on this system. `name` must be an existing IMS Authorization Service and be from 1 to 63 alpha and/or numeric characters.

```imsi id```
Disconnects the subscriber with the specified id. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘ '). For example; ‘$’.

```ip-alloc-method {aaa-assigned | dhcp [ relay-agent | proxy-client ] | dynamic-pool | 12tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }```
Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:

- `aaa-assigned`: Selects subscribers whose IP Addresses were assigned by AAA.
### Exec Mode Commands (A-C)

- **clear subscribers**
  -Disconnects all subscribers connected to the specified **ip_address**. The address must be specified using the standard IPv4 dotted decimal notation.

- **ip-pool name**
  -Disconnects all subscribers assigned addresses from the IP address pool **pool_name**. **pool_name** must be the name of an existing IP pool or IP pool group.

- **ipv6-address address**
  -Clears all subscribers connected to the specified IPv6 **address**.

- **ipv6-prefix prefix**
  -Clears subscribers from a specific IPv6 address prefix.

- **lac address**
  -Disconnects all calls to the peer LAC (L2TP access concentrator) specified by **address**. The address must be specified using the standard IPv4 dotted decimal notation.

- **lac-service name**
  -Disconnects all calls for this LAC service. **name** is a string of 1 to 63 characters.

- **lma-service name**
  -Disconnects subscribers using this LMA service configured on this system. **name** must be an existing LMA service and be from 1 to 63 alpha and/or numeric characters.

- **lns address**
  -Disconnects calls to the peer LNS (L2TP network server) specified by **address**. The address must be specified using the standard IPv4 dotted decimal notation.
clear subscribers

**lns-service name**
Disconnects calls associated with the LNS service named *name*. *name* is a string of 1 to 63 characters.

**long-duration-time-left [ < | > | greater-than | less-than ] value**
Disconnects subscriber sessions whose time left for the maximum duration of their session matches the length of time specified.
- `<`: Filters output so that only information less than the specified value is cleared.
- `>`: Filters output so that only information greater than the specified value is cleared.
- `greater-than`: Filters output so that only information greater than the specified value is cleared.
- `less-than`: Filters output so that only information less than the specified value is cleared.
- `value`: If no other filtering options are specified only output matching `value` is cleared. If `value` is not specified all data is cleared. `value` must be an integer from 0 through 4294967295.

**mag-service name**
Disconnects subscribers using this Mobile Access Gateway (MAG) service configured on this system. *name* must be an existing MAG service and be from 1 to 63 alpha and/or numeric characters.

**mip-udp-tunnel-only**
This option clears the subscribers that negotiated MIP-UDP tunneling with the HA. This option is only valid when MIP NAT Traversal license is enabled.

**mme-address ipv4_addr**
Disconnects subscribers using this peer Mobility Management Entity (MME). *ipv4_addr* must be an existing peer MME IPv4 address and be specified in dotted decimal notation.

**mme-only**
Disconnects all MME subscriber sessions on the system.

**mme-service name**
Disconnects subscribers using this MME service configured on this system. *name* must be an existing MME service and be from 1 to 63 alpha and/or numeric characters.

**msid id**
Disconnects the mobile user identified by *ms_id*. *ms_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘’). For example; ‘$’.

In case of **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers supplied, this filter will clear subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.

**clear subscribers msid 111110123456789 or**
**clear subscribers msid 0123456789**
will clear any subscriber with a MSID that match the lower 10 digits of MSID supplied, i.e. 0123456789.

**msisdn msisdn**
Clears information for the mobile user identified by Mobile Subscriber ISDN Number (MSISDN). *msisdn* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.
clear subscribers

```
exec { not-required | required [ nat-ip nat_ip_address | nat-realm nat_realm ] }
```

Clears all subscriber information for the specified subscribers:

- **not-required**: Subscribers for whom NAT processing is not required.
- **required**: Subscribers for whom NAT processing is required.

**Important**: The **nat-ip** keyword is only available in StarOS 8.3 and later.

- **nat-ip nat_ip_address**: Subscribers for whom NAT processing is enabled and are using the specified NAT IP address. `nat_ip_address` specifies the NAT IP address and must be a standard IPv4 address.
- **nat-realm nat_realm**: Subscribers for whom NAT processing is enabled and are using the specified NAT realm. `nat_realm` specifies the NAT realm name and must be a string from 1 through 63 characters in length.

**network-requested**

Disconnect subscriber sessions that were initiated by the GGSN network requested create PDP context procedure.

```
network-type { gre | ipv4 | ipv6 | ipip | l2tp | mobile-ip | proxy-mobile-ip }
```

Disconnects subscriber sessions based on the network type. The following network types can be selected:

- **gre**: Generic Routing Encapsulation (GRE) per RFC 2784
- **ipv4**: Internet Protocol version 4 (IPv4)
- **ipv6**: Internet Protocol version 6 (IPv6)
- **ipip**: IP-in-IP encapsulation per RFC 2003
- **l2tp**: Layer 2 Tunneling Protocol encryption per RFC 2661
- **mobile-ip**: Mobile IP
- **proxy-mobile-ip**: Proxy Mobile IP

```
exec { < | > | less-than | greater-than } ipv4_address [ [ < | > | less-than | greater-than ] ipv4_address ]
```

Displays information for subscribers connected via the packet control function with a specific or range of IP address `ipv4_address`. The address must be specified using the standard IPv4 dotted decimal notation.

- `<`: Filters output so that only information less than the specified IPv4 address value is displayed.
- `>`: Filters output so that only information greater than the specified IPv4 address value is displayed.
- `less-than`: Filters output so that only information less than the specified IPv4 address value is displayed.
- `greater-than`: Filters output so that only information greater than the specified IPv4 address value is displayed.

**Note**: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

```
pdsn-service name
```

Disconnect all subscribers connected to the packet data service `pdsn_name`. The packet data service must have been previously configured.
clear subscribers

**pdg-service service_name**

Disconnects subscriber sessions that are using the PDG service.

*service_name* must be an existing service and be from 1 to 63 alpha and/or numeric characters.

**pdif-service service_name**

Clears counters for subscribers accessing the Packet Data Interworking Function (PDIF) service.

*service_name* must be an existing service and be from 1 to 63 alpha and/or numeric characters.

**pgw-only { all | imsi id ebi id | pgw-service name | sgw-address ipv4_addr }**

- **all**: Disconnects all subscribers for all P-GW services on this system.
- **imsi id ebi id**: Disconnects subscribers based on their International Mobile Subscriber Identification (IMSI). *id* must be the 3 digit MCC (Mobile Country Code), follow by the 2 or 3 digits of the MNC (Mobile Network Code) and the MSIN (Mobile Subscriber Identification Number). *id* should not exceed 15 digits. Example: 123-45-678910234 must be entered as 12345678910234
- The EBI (EPS Bearer Identity) *id* must be a valid EBI and be an integer value from 5 to 15.
- **pgw-service name**: Disconnects all subscribers using this P-GW service. *name* must be an existing P-GW service and be from 1 to 63 alpha and/or numeric characters.
- **sgw-address ipv4_addr**: Disconnects all subscribers using this S-GW IP address. *ipv4_addr* must be an existing IPv4 address and be specified in dotted-decimal notation.

**plmn-type { home | roaming | visiting }**

For GGSN, disconnect subscribers whose subscriber type matches the specified type.

**qci { number }**

Disconnects subscribers based on their QCI identity. *number* must be an integer value from 0 to 9.

**rx-data [ < | > | greater-than | less-than ] value**

Disconnects subscribers who have received the specified number of bytes of data.

- `<`: Filters output so that only information less than the specified value is cleared.
- `>`: Filters output so that only information greater than the specified value is cleared.
- **greater-than**: Filters output so that only information greater than the specified value is cleared.
- **less-than**: Filters output so that only information less than the specified value is cleared.

*value*: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 18446744073709551615.

**s5proto { gtp | pmip }**

Disconnects subscribers based on their S5 interface protocol type.

- **gtp**: Indicates that the GTP protocol is used on the S5 interface for the subscribers being disconnected.
- **pmip**: Indicates that the PMIP protocol is used on the S5 interface for the subscribers being disconnected.

**session-time-left [ < | > | greater-than | less-than ] value**

The amount of time left for the subscriber session.

- `<`: Filters output so that only information less than the specified value is cleared.
- `>`: Filters output so that only information greater than the specified value is cleared.
- **greater-than**: Filters output so that only information greater than the specified value is cleared.
- **less-than**: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching value is cleared. If value is not specified all data is cleared. value must be an integer from 0 through 4294967295.

sgsn-address address
Clears all PDP contexts currently being facilitated by a specific SGSN.
address is the IP address of the SGSN expressed in dotted decimal notation.

sgsn-service name
Clears all PDP contexts associated with SGSN. This keyword can be used with filtering keywords that are part of the clear subscriber command set.
Using this keyword can trigger a network-initiated service request (paging) procedure.
name is the identity of a specific SGSN-service configuration. The name consists of 1 to 63 alphanumeric characters.

sgw-only
Disconnects all S-GW subscriber sessions on the system.

sgw-service name
Disconnects subscribers using this Serving Gateway (S-GW) service configured on this system. name must be an existing S-GW service and be from 1 to 63 alpha and/or numeric characters.

tx-data [ < | > | greater-than | less-than ] value
Disconnects subscribers who have transmitted the specified number of bytes of data.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching value is cleared. If value is not specified all data is cleared. value must be an integer from 0 through 18446744073709551615.

username name
Disconnect the subscriber with the specified username
name is the username of the subscriber to be cleared. name must be a sequence of characters and/or wildcard characters (‘$’ and ‘*’) from 1 to 127 characters in length. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘‘). For example; ‘$’.

verbose
Indicates the output should provide as much information as possible. If this option is not specified then the output is the standard level which is the concise mode.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.
Usage
Clear subscribers sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be useful when preparing for maintenance activities such that connects may be cleared to perform any necessary procedures.

Example
The following examples illustrate the basic command usage as well as the redirection of the command output. Not all options are exemplified as all options follow the same basic constructs.
The following are basic subscriber clearing examples.

```
clear subscribers username user1
```
```
clear subscribers ha sampleService
```
```
clear subscribers ip-pool poolName verbose
```

The following command disconnects users connected to the foreign agent with IP address 1.2.3.4.
```
clear subscribers fa 1.2.3.4
```

The following redirects the output of the command to the more command for paging of the output to allow easier viewing of all output by the user. This example highlights the use of the verbose option as well.
```
clear subscribers all verbose | more
```
clear super-charger

Deletes the subscriber’s backed-up subscription data.

Product
SGSN

Privilege
Administrator, Security Administrator

Syntax

```
clear super-charger { imsi | all }
```

**imsi**
Defines a specific subscriber’s international mobile subscriber identity (IMSI) number.

- **imsi**: up to 15 digits. This number includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number).

**all**
Instructs the SGSN to delete subscription data for all super charger subscribers.

Usage
Use this command to clear (delete) the subscription data records for one or all subscribers with super charger subscription configuration.

Example
The following command deletes the backed up records for the subscriber identified by the IMSI 90121882144672.

```
clear super-charger imsi 90121882144672
```
cli

This command specifies command line interface (CLI) session behavior

Product
All

Privilege
Security Administrator, Administrator, Operator, inspector

Syntax

cli { history | stop-on-first-error }

no cli { history | stop-on-first-error }

no
Disables the specified keyword functionality.

history
Default: Enabled
Enables command line history for the current command line session.

stop-on-first-error
Default: Disabled
When this is enabled, when a configuration file is loaded, on the first syntax error the system stops loading the configuration file.

Usage
This command controls CLI settings pertaining to the maintenance of a per-session command history and syntax error monitoring during configuration file loading.
By default, the system maintains a list of commands executed during each CLI session. This list is referred to as a history.
In addition, the system can be configured to stop loading a configuration if a syntax error is detected. By default, the system identifies the error but continues to process the configuration file.

Example
The following command disables the keeping of a CLI history for the current session:

no cli history
**clock set**

Sets the system time.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
clock set date_time
```

*date_time*

Specifies the date and time to set the system clock. Specified as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where YYYY is a 4-digit year, MM is a 2-digit month in the range 01 through 12, DD is a 2-digit day in the range 01 through 31, HH is a 2-digit hour in the range 00 through 23, mm is a 2-digit minute in the range 00 through 59, and ss is a 2-digit second in the range 00 through 59.

**Usage**

Set the clock to adjust the system clock for such things as timing drift, day-light savings adjustment, etc. New settings are immediately applied to all CPUs in the system.

**Important:** This command should only be used if there is no NTP server enabled for any context. If NTP is running on the system, this command returns a failure.

**Example**
The following commands set the system clock where one sets the exact second as well.

```
clock set 2003:08:23:02:30
```

```
clock set 2003:08:23:02:30:30
```
configure

Sets the mode to the global configure mode. May also be used to set the mode to the configure mode and pre-load the configuration referred to by the options.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
configure [ url [ verbose ] ]
```

- **url**
  Specifies the location of a configuration file to pre-load. url may refer to a local or a remote file. url must be entered using one of the following formats:
    - ASR 5000:
      - `[ file: ]{ /flash | /pcmcia | /hd } [ /directory ]/file_name`
      - `tftp://[ host[ :port# ] ] [ /directory ]/file_name`
      - `[ http: | ftp: | sftp: ]///[ username [ :password ] @ ] [ host ] [ :port# ] [ /directory ]/file_name`

**Important:** Use of the SMC hard drive is not supported in this release.

- **directory** is the directory name.
- **filename** is the actual file of interest.
- **username** is the user to be authenticated.
- **password** is the password to use for authentication.
- **host** is the IP address or host name of the server.
- **port#** is the logical port number that the communication protocol is to use.

- **verbose**
  Displays each the line number and actual line content from the configuration as it is processed.

Usage
If no URL is specified, executing this command causes the CLI to enter the Global Configuration Mode. If a URL is specified, executing this command loads the specified configuration file.

Example
The following simply changes the mode to the command line interface global configuration mode.

```
configure
```
The following command loads a configuration file from the node `sampleNode` given the path specified and a local file, respectively.

```
configure ftp://sampleNode/pub/glob.cfg
configure /pcmcia/pub/glob.cfg verbose
```
context

Sets the current context to the context specified.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

context name

name

Specifies the context of interest. Must be a previously defined context.

Usage
Change the current context when it is desired to configure and/or manage a specific context.

Example
The following sets the current context to the sampleContext context.

context sampleContext
**copy**

Copies files from one location to another. Allows files to be copied to/from locally as well as from one remote location to another.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
copy from_url to_url [ passive ] [ -noconfirm ]
```

**from_url**

Specifies the source of the copy. `url` may refer to a local or a remote file. `url` must be entered using one of the following formats:

- **ASR 5000:**
  - `[file: ]{/flash|/pcmcia1|/hd}[ /directory ]/file_name`
  - `tftp://{ host[ :port# ]}{ /directory ]/file_name`
  - `{ http: | ftp: | sftp: }///{ username[ :password ]@ }{ host }[ :port# ]{ /directory ]/file_name`

**Important:** Use of the SMC hard drive is not supported in this release.

- `directory` is the directory name.
- `filename` is the actual file of interest.
- `username` is the user to be authenticated.
- `password` is the password to use for authentication.
- `host` is the IP address or host name of the server.
- `port#` is the logical port number that the communication protocol is to use.

**to_url**

Specifies the destination of the copy. `url` may refer to a local or a remote file. `url` must be entered using one of the following formats:

- **ASR 5000:**
  - `[ file: ]{/flash | /pcmcia1 | /hd}[ /directory ] /file_name`
  - `tftp://{ host[ :port# ] }{ /directory ] /file_name`
  - `{ ftp: | sftp: } / / { username [ :password ] @ } { host }[ :port# ]{ /directory ] /file_name`

**Important:** Use of the SMC hard drive is not supported in this release.

- `directory` is the directory name.
- `filename` is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

passive
Indicates the file copy is to use the passive mode.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Important: Use of the -noconfirm option allows the over writing of an existing file if the destination file already exists.

Usage
Copy configuration files, log files, etc., to provide backups of data through the network.

Example
The following copies files from the local /flash/pub directory to remote node remoteABC's /pcmcia2/pub directory with and without confirmation respectively.

    copy http://remoteABC/pub/june.cfg /flash/pub/june.cfg
    copy tftp://remoteABC/pub/june.cfg /pcmcia2/pub/june.cfg -noconfirm

The following copies files from remote node remoteABC to remote node remote123.

    copy ftp://remoteABC/pub/may.cfg ftp://remote123/pub/may.cfg
crash copy

Copies individual crash files (one-at-a-time) and optionally the core dump file from the stored crash records on the chassis to a user-specified location.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
    crash copy number number url to_url [ core ]
```

**number number**

The identification number of the crash record. *number* must be an integer representing a valid record number selected from a range of 1 to 120. To determine the numeric identity of a specific crash file, use the `show crash list` command in Exec mode.

**url to_url**

Specifies the destination of the copy. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats:

- ASR 5000:
  ```
  • tftp://[ host[ :port# ] ] [ /directory ] /
  • [ ftp: | sftp: ]://[ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /
  ```

**Important:** Use of the SMC hard drive is not supported in this release.

*directory*: the name of the target directory.
*username*: the username to be authenticated to provide access to targeted server.
*password*: the username’s password to be authenticated.
*host*: the IP address or host name of the targeted server.
*port#*: the number of the target server’s logical port used for the selected communication protocol.

**Important:** Do not specify a target filename as this will prevent the file from writing to the target server. The system generates and provides a timestamp-based filename that appears at the destination when the copy command completes.

**core**

Including this keyword as part of the command instructs the system to copy the core dump to the targeted storage server. The core cannot be copied alone; it must be part of a `crash copy` action included when copying a crash file.
Usage

Copy crash files of core dump to another location for backup or analysis.

Example

The following uses `ftp` to copy stored record number 5 and the core dump from the crash record list to a targeted remote node directory called `crasharchive` through port 22 of the targeted server `remoteABC` with access through user `homeboy` whose password is `secret.7.word`.

```
crash copy number 5 url ftp://homeboy:secret.7.word@remoteABC:22/crasharchive/core
```
crypto-group

Allows the manual switchover of redundant IPSec tunnels belonging to a specific crypto group.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

crypto-group name group_name activate { primary | secondary }

group_name

*group_name* is the name of the crypto group to which the tunnels to be switched are associated.

**activate { primary | secondary }**

Allows you to specify which tunnel to activate (i.e. to facilitate user traffic):

*• primary*: Switch traffic to the primary tunnel in the group.

*• secondary*: Switch traffic to the secondary tunnel in the group.

**Usage**

This command is used in conjunction with the Redundant IPSec Tunnel Fail-over feature. Use this command to manually switch traffic to a specific tunnel in a crypto group if the automatic switchover options have been disabled. Refer to the *switchover* command in the Crypto Group configuration mode for more information.

**Example**

The following command manually switches user traffic to the secondary tunnel in the crypto group called *group1*:

crypto-group group1 activate secondary
Chapter 90
Exec Modes Commands (D-S)

This chapter contains the commands in the Exec Mode from debug to sgsn offload.
The following commands send information to the logging facility for review:

**debug ip**

Enables/disables the debug options for IP debugging. If logging is enabled, results are sent to the logging system.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
debug ip { arp | interface | route }
no debug ip { arp | interface | route }
```

- **no**
  Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

- **arp | interface name | route**
  Specifies which IP interfaces/function to debug.
  - **arp**: indicates debug is to be enabled for the address resolution protocol.
  - **interface**: indicates debug is to be enabled for the IP interfaces.
  - **route**: indicates debug is to be enabled for the route selection and updates.

**Usage**
The debug IP command is valuable when troubleshooting network problems between nodes. The debugging is stopped by using the `no` keyword.

⚠️ **Caution:** Issuing this command could negatively impact system performance depending on system configuration and/or loading.

**Example**
The following commands enable/disable debugging for ARP.

```
debug ip arpnof debug ip arn
```

The following enables/disables debugging for IP interfaces.

```
debug ip interface
no debug ip interface
```

The following enables/disables debugging for routing.

```
debug ip routenof debug ip route
```
debug ip bgp

This command enables BGP debug flags. If logging is enabled, results are sent to the logging system.

Product
HA

Privilege
Security Administrator, Administrator, Operator

Syntax

dbg ip bgp {all | event | filters | fsm | keepalives | updates { inbound | outbound } }

no debug ip bgp { all | event | filters | fsm | keepalives | updates { inbound | outbound } }

Usage
Use this command to enable or disable BGP debug flags.

Example
The following command disables all BGP debug flags enabled by any of the debug ip bgp commands:

```plaintext
no debug ip bgp all
```

The following command enables all BGP debug flags:

```plaintext
d-debug ip bgp all
```
**debug ip ospf all**

This command enables all OSPF debug flags. If logging is enabled, results are sent to the logging system.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
debug ip ospf all
no debug ip ospf all
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disable all OSPF debug flags.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable or disable all OSPF debug flags.

**Example**

The following command disables all OSPF debug flags enabled by any of the `debug ip ospf` commands:

```
no debug ip ospf all
```

The following command enables all OSPF debug flags:

```
ddebug ip ospf all
```
**debug ip ospf event**

This command enables debugging of OSPF protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
debug ip ospf event [ abr | asbr | vl | lsa | os | router ]
```

```
no debug ip ospf event [ abr | asbr | vl | lsa | os | router ]
```

**Usage**
Use this command to output debug information for OSPF events.

**Example**
To enable all event debug information, enter the following command;

```
diag ip ospf event
```
To disable all event debug information, enter the following command:

```
no debug ip ospf event
```
**debug ip ospf ism**

This command enables OSPF Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
debug ip ospf ism [ events | status | timers ]
no debug ip ospf ism [ events | status | timers ]
```

- **events**
  Enable debugging ISM event information.

- **status**
  Enable debugging ISM status information.

- **timers**
  Enable debugging ISM timer information.

**Usage**

Use this command to output ISM debug information.

**Example**

To enable all ISM debug information, enter the following command:

```
debug ip ospf ism
```

To disable all ISM debug information, enter the following command:

```
no debug ip ospf ism
```
debug ip ospf lsa

This command enables troubleshooting on OSPF Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
debugip ospf lsa [ flooding | generate | install | refresh | maxage | refresh ]
no debugip ospf lsa [ flooding | generate | install | refresh | maxage | refresh ]
```

---

**no**
Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

---

**flooding**
Enable LSA flooding information.

---

**generate**
Enable LSA generation information.

---

**install**
Enable LSA install information.

---

**maxage**
Enable LSA maxage information in seconds. The maxage is equal to 3600 seconds.

---

**refresh**
Enable LSA refresh information.

---

**Usage**

Use this command to output debug information for LSAs.

---

**Example**

To enable all LSA debug information, enter the following command;

```plaintext
debug ip ospf lsa
```

To disable all LSA debug information, enter the following command;

```plaintext
no debug ip ospf lsa
```
no debug ip ospf lsa
debug ip ospf nsm

This command enables troubleshooting OSPF Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
debug ip ospf nsm [ status | events | timers ]
nodebug ip ospf nsm [ status | events | timers ]
```

- **no**
  Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

- **events**
  Enables debugging NSM event information.

- **status**
  Enables debugging NSM status information.

- **timers**
  Enables debugging NSM timer information.

**Usage**
Use this command to output debug information for OSPF NSMs.

**Example**
To enable all NSM debug information, enter the following command;

```
debug ip ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ip ospf nsm
```
**debug ip ospf packet**

This command enables troubleshooting of specific OSPF packet information. If logging is enabled, results are sent to the logging system.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
debug ip ospf packet { all | dd | hello | ls-ack | ls-request | ls-update } [ send | recv ] [ detail ]
```

```
nodebug ip ospf packet { all | dd | hello | ls-ack | ls-request | ls-update } [ send | recv ] [ detail ]
```

---

**no**

Disable debugging of the specified packet information.

---

**all**

Enable debugging all OSPF packet information.

---

**dd**

Enable debugging database descriptions.

---

**hello**

Enable debugging hello packets.

---

**ls-ack**

Enable debugging link state acknowledgements.

---

**ls-request**

Enable debugging link state requests.

---

**ls-update**

Enable debugging link state updates.

---

**send**

Enable debugging only on sent packets.

---

**recv**

Enable debugging only on received packets.
**debug ip ospf packet**

---

**detail**

Enable detailed information in the debug output.

---

**Usage**

Use this command to output specific OSPF packet information.

---

**Example**

To enable all packet debug information, enter the following command:

```
debug ip ospf packet all
```

To disable all route debug information, enter the following command:

```
no debug ip ospf packet all
```
**debug ip ospf route**

This command sets the route calculation method to use in debugging OSPF routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
debugipospfroute [ ase | ia | install | spf ]
nodebugipospfroute [ ase | ia | install | spf ]
```

- **no**
  Disables debugging of route information. If no keyword is specified all information types are disabled.

- **ase**
  Enables debugging information on external route calculations.

- **ia**
  Enables debugging information on Inter-Area route calculations.

- **install**
  Enables debugging information on route installation.

- **spf**
  Enables debugging information on SPF route calculations.

**Usage**

Use this command to output debug information for OSPF routes.

**Example**

To enable all route debug information, enter the following command;

```
d debug ip ospf route
```

To disable all route debug information, enter the following command;

```
no debug ip ospf route
```
**debug ip ospf router**

This command sets the debug option for OSPF router information. If no keyword is specified, all router information is enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
debug ip ospf router [ interface | redistribute ]
```

```
no debug ip ospf router [ interface | redistribute ]
```

- **no**
  - Disables the specified router debug information. If no keyword is specified, all router information is disabled.

- **interface**
  - Enables router interface information.

- **redistribute**
  - Enables router redistribute information.

**Usage**

Use this command to output debug information for the OSPF router.

**Example**

To enable all router debug information, enter the following command:

```
debug ip ospf router
```

To disable all router debug information, enter the following command:

```
no debug ip ospf router
```
default terminal

Restores the system default value for the terminal options.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

default terminal { length | width }

length | width
length: reset the terminal length to the system default.
width: restores the system default terminal width.

Usage
Restore the default terminal settings when the current paging and display wraps inappropriately or pages to soon.

Example
The following sets the default length then width in two commands.

default terminal length

default terminal width
delete

Removes the specified file(s) permanently from the local.

Product
All

Privilege
Security Administrator, Administrator

Syntax

dele**te** filepath [ -noconfirm ]

filepath
Specifies the location of the file to delete. The path must be formatted according to the following format:

| Specifies the source of the copy. url may refer to a local or a remote file. url must be entered using one of the following formats: |
| ASR 5000: |
| ![Important](image) Use of the SMC hard drive is not supported in this release. |
| directory is the directory name |
| filename is the actual file of interest |

-`-noconfirm`
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Important**: Use of the `-noconfirm` option should be done with extra care to ensure the file is specified accurately as there is no method of recovering a file that has been deleted.

Usage
Deleting files is a maintenance activity which may be part of periodic routine procedures to reduce system space utilization.

Example
The following removes files from the local `flash/pub` directory.

`delete /flash/pub/june03.cfg`
**dhcp force**

Tests the lease-renewal for DHCP-assigned IP addresses for a particular subscriber.

**Product**

GGSN, ASN-GW

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
dhcp force lease-renewal { callid id | imsi imsi [ nsap nsapi ] | msid msid }
```

- **callid id**
  
  Clears the call specified by `call_id`. The call ID must be specified as a 4-byte hexadecimal number.

- **imsi msid**
  
  Disconnects the subscriber with the specified msid. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘‘). For example; ‘$’.

- **nsapi nsapi**
  
  A specific Network Service Access Point Identifier (NSAPI). `nsapi` is an integer value from 5 to 15.

- **msid id**
  
  Disconnects the mobile user identified by `ms_id`. `ms_id` must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘‘). For example; ‘$’.

**Usage**

Use this command tests a forced IP address lease renewal for a specific subscriber.

**Example**

The following command tests DHCP lease renewal for a subscriber with an MSID of 1234567:

```
dhcp force lease-renewal msid 1234567
```
**dhcp test**

Tests DHCP functions for a particular DHCP service.

**Product**
GGSN, ASN-GW

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
dhcp test dhcp-service svc_name [ all | server ip_address ]
```

- `dhcp-service svc_name`
  The name of the DHCP service. It can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.

- `all`
  Tests DHCP functionality for all servers.

- `server ip_address`
  Tests DHCP functionality for the server.
  `ip_address` is the IP address of the DHCP server in dotted-decimal notation.

**Usage**

Once DHCP functionality is configured on the system, this command can be used to verify that it is configured properly and that it can successfully communicate with the DHCP server. Executing this command causes the system to request and allocate an IP address and then release it. If a specific DHCP server is not specified, then each server configured in the service is tested.

**Example**

The following command tests the system's ability to get an IP address from all servers a DHCP service called DHCP-Gi is configured to communicate with:

```
dhcp test dhcp-service DHCP-Gi all
```

The following displays a sample of this command's output showing a successful DHCP test.

```
DHCP test status for service <DHCP-Gi>: Server address: 192.168.16.2 Status: 
Tested Lease address: 192.168.16.144 Lease Duration: 600 secs.
```


**diameter disable endpoint**

This command disables a diameter peer without removing the peer’s configuration.

**Product**

PDIF, SCM

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
diameter disable endpoint endpoint_name peer peer_id
```

- **endpoint endpoint_name**
  Specifies the endpoint in which the peer is configured.  
  `endpoint_name` must be the endpoint name, and must be a string of 1 through 63 characters in length.

- **peer peer_id**
  Specifies the peer to be disabled.  
  `peer_id` must be the diameter peer host name, and must be a string of 1 through 63 characters in length.

**Usage**

Use this command to administratively disable a diameter peer without removing the peer configuration. This command will tear down all connections on the specified peer (by sending a DPR if the configuration demands the same at peer level configuration). The peer will remain in disabled state until it is enabled again. Also see the `diameter enable endpoint` command.

**Example**

This command disables the diameter peer `peer12`:

```plaintext
diameter disable endpoint endpoint1 peer peer12
```
diameter enable endpoint

This command enables a diameter peer that is disabled.

Product
PDIF, SCM

Privilege
Security Administrator, Administrator

Syntax

diameter enable endpoint endpoint_name peer peer_id

endpoint endpoint_name
Specifies the endpoint in which the peer is configured.
endpoint_name must be the endpoint name, and must be a string of 1 through 63 characters in length.

peer peer_id
Specifies the peer to be enabled.
peer_id must be the diameter peer host name, and must be a string of 1 through 63 characters in length.

Usage
Use this command to administratively enable a diameter peer. Also see the diameter disable endpoint command.

Example
This command enables the diameter peer peer12:

diameter enable endpoint endpoint1 peer peer12
diameter reset connection

This command resets individual TCP/SCTP connections.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
diameter reset connection { endpoint endpoint_name peer peer_id }
```

- **endpoint endpoint_name**
  Resets connection to the specified endpoint.
  *endpoint_name* must be the endpoint name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **peer peer_id**
  Resets connection to the specified peer.
  *peer_id* must be the Diameter peer host name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage

Use this command to reset the TCP/SCTP connections for the specified endpoint/peer. With this command, the connection will be closed temporarily after DPR/DPA. If there is any traffic to be sent to the particular peer, then the connection will be re-established.

This command overrides the endpoint configured in any other configuration mode.

This command is applicable only when the specified peer is enabled.

Example

This command resets connection to the specified endpoint:

```
diameter reset connection endpoint <endpoint_name>
```
diameter reset route failure

This command resets the failed route status of Diameter destination-host combination via peer to AVAILABLE status.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
diameter reset route failure [ endpoint endpoint_name ] [ host host_name ] [ peer peer_id ]
```

**endpoint endpoint_name**
Resets paths to the specified endpoint.
endpoint_name must be a string of 1 through 63 characters in length.

**host host_name**
Resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis having a specific host name to AVAILABLE.
host_name must be the Diameter host name, and must be a string of 1 through 63 characters in length.

**peer peer_id**
Resets the FAILED status of all Diameter destination-host combination routes via a peer having specific peer-id for every Diameter client within the chassis to AVAILABLE.
peer_id must be the Diameter peer host name, and must be a string of 1 through 63 characters in length.

Usage
Use this command to reset the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis to AVAILABLE status.
This command also resets the failure counts used to determine the AVAILABLE/FAILED status of destination-host combination.
When executed from local context, this command matches all contexts. If an optional keyword is not supplied, a wildcard is used for the value.
The status of every matching combination of destination-host via peer for every matching Diameter client within the chassis will be reset to AVAILABLE. The failure counts that are used to determine AVAILABLE/FAILED status will also be reset.
Also see the route-entry and route-failure CLI commands in the Diameter Endpoint Configuration Mode.
Default value: N/A

Example
The following command resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis for specified endpoint name to AVAILABLE.
diameter reset route failure endpoint endpoint_name
directory

Lists the files in a specified location.

Product
All

Privilege
Security Administrator, Administrator

Syntax

directory filepath [ -size ] [ -reverse ] [ -time ]

filepath
Specifies the directory path to list the contained files. The path must be formatted according to the following format:
Specifies the source of the copy. url may refer to a local or a remote file. url must be entered using one of the following formats:
• ASR 5000:
  * [ file: ] { /flash | /pcmcia1 | /hd } [ /directory ] /file_name

Important: Use of the SMC hard drive is not supported in this release.

directory is the directory name
filename is the actual file of interest

-size
Indicates the size of each file should be displayed in the output.

-reverse
Indicates the order of files listed should be in descending order (z-aZ-A9-0). Default is to sort in ascending order (0-9A-Za-z).

-time
Indicates the last modification timestamp of each file should be displayed in the output.

Usage
Lists such things as log and crash files from multiple nodes within the network.
The optional arguments may be specified individually or in any combination.

Example
The following command will list the files in the local /flash/pub directory sorted in reverse order.

directory /flash/pub -reverse
disable

Prevents the system from making requests of a selected RADIUS server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
disable radius [ accounting | charging [ accounting ] ] server address [ port num ] [ group name ]
```

**accounting | charging | charging accounting**

Specifies the type of RADIUS server to disable.

**server address**

Identifies the RADIUS server by IP address.

`address` is specified using the standard IPv4 or IPv6 dotted decimal notation.

**port num**

Default: 1812 (authentication) 1813 (accounting)

Specifies the port number of the RADIUS server being disabled.

`num` must be the configured port number of the RADIUS server being disabled and be 0 to 65535 numeric characters in length.

**group name**

Default: default

Specifies the RADIUS group to which the server belongs. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group.

`name` must be the name of a configured RADIUS Server group and be 1 to 63 characters in length.

**Usage**

Use this command to gracefully stop the system from making requests of a specific RADIUS server.

**Example**
The following command disables a RADIUS accounting server with an IP address of 1.2.3.4, the default accounting server port number, and that resides in the “Group5” server group:

```
disable radius accounting server 1.2.3.4 group Group5
```
**dns-client**

This command performs DNS query on the basis of specified DNS client name, DNS query domain name, and type of query criteria.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

dns-client  dns_client_name  [  query-type  {  A  |  AAAA  |  NAPTR  |  SRV  }  ]  query-name

**Example**
The following command displays statistics for a DNS client named test_dns with query type for IP address as A and query name as domain1.com

dns-client  test_dns  query-type  A  query-name  domain1.com
dns-client
enable

Allows the system to start making requests of a selected RADIUS server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
enable radius [ accounting | charging | [ accounting ] ] server address [ port num ] [ group name ]
```

<table>
<thead>
<tr>
<th>accounting</th>
<th>charging</th>
<th>charging accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the type of RADIUS server to enable.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>server address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the RADIUS server by IP address.</td>
</tr>
</tbody>
</table>

| address is specified using the standard IPv4 or IPv6 dotted decimal notation. |

<table>
<thead>
<tr>
<th>port num</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 1812 (authentication) 1813 (accounting)</td>
</tr>
<tr>
<td>Specifies the port number of the RADIUS server being enabled.</td>
</tr>
</tbody>
</table>

| num must be the configured port number of the RADIUS server being enabled and must be 0 to 65535 numeric characters in length. |

<table>
<thead>
<tr>
<th>group name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: default</td>
</tr>
<tr>
<td>Specifies the RADIUS group to which the server belongs. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group.</td>
</tr>
</tbody>
</table>

| name must be the name of a configured RADIUS Server group and be 1 to 63 characters in length. |

Usage
Use this command to allow the system to start making requests of a specific RADIUS server.

Example
The following command enables a RADIUS accounting server with an IP address of 1.2.3.4, the default accounting server port number, and that resides in the “Group5” server group:

```
enable radius accounting server 1.2.3.4 group Group5
```
exit

Exits the current CLI session.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

exit

Usage
Use this command to close the current CLI session.
filesystem format

Used to format the PCMCIA card or the Compact Flash on the SMC.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ASR 5000:

filesystem format { /flash | /pcmcia1 | /hd } [ othersmc ]
```

{ /flash | /pcmcia1 | /pcmcia2} or { /flash | /pcmcia1 | /hd }

Format the file system on the specified device.

**Important:** Use of the SMC hard drive is not supported in this release.

```
[ othersmc ]
```

Format the file system on the standby SMC.

**Usage**
Clear all directories and files from the PCMCIA card(s) and/or the Compact Flash and re-establish the file system.

**Example**
The following command formats the PCMCIA card located in slot 1 on the SMC:

```
filesystem format /pcmcia1
```
filesystem repair

Used to repair the file system on a PCMCIA card or the Compact Flash on the SMC.

Product
All

Privilege
Security Administrator, Administrator

Syntax
ASR 5000:

```
filesystem repair {/flash | /pcmcia1 | /pcmcia2 | /hd} [checkonly] [othersmc]
```

Repair the file system on the specified device.

**Important:** Use of the SMC hard drive is not supported in this release.

```
[ checkonly ]
Check, but do not repair, the file system.

[ othersmc ]
Repair the file system on the standby SMC.
```

Usage
Repair the file system on a PCMCIA card or the Compact Flash.

Example
The following command repairs the file system on the PCMCIA card located in slot 1 on the SMC:

```
filesystem format /pcmcia1
```
**gtpc test echo**

Tests the ability of a GGSN service to exchange GTP-C echo request messages with the specified SGSN(s).

**Product**
GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
  gtpc test echo src-address gn_address { all | sgsn-address ip_address }
```

- **src-address** `gn_address`
  Specifies the IP address of a Gn interface configured on the system.
  `gn_address` must be expressed in dotted decimal notation.

- **all**
  Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.

- **sgsn-address** `ip_address`
  Specifies that GTP-C echo requests will be sent to a specific SGSN.
  `ip_address` is the address of the SGSN to send the requests to and must be expressed in dotted decimal notation.

**Usage**

This command tests the GGSN’s ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring. This command must be executed from within the context in which the GGSN service is configured. Refer also to the `gtpu test` command.

**Example**

The following command issues GTP-C echo packets from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2:

```
  gtpc test echo src-address 192.168.157.32 sgsn-address 192.168.157.2
```

The following displays a sample of this command’s output.

```
GTPC test echo-------------------SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 1 (COMPLETE) Recovery: 202 (0xCA)
```
gtpc test echo
gtppp interim now

Check points current GTPP accounting messages and identifies which types of interim CDRs are to be generated and sent to the external charging/storage servers (e.g., a CFG or a GSS). The impact of this command is immediate.

**Product**

GGSN, SGSN

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
gtppp interim now (active-charging egcdr|apnapn_name| calldcall_id|cdr-types ( gcdr | mcdr | scdr | dhcp-serverip_address|gprs-servicesvc_name| ggsn-servicesvc_name| imsiimsi[ ip-addresssub_address[ username| username] now | nsapsnsapi[ ip-addresssub-address[ username| username] ] | ip-addresssub_address[ username| username] ] | ip-poolpool_name|mccmcc_number|mncmnc_number|msisdnmsisdn_num|sgsn-addressip_address|sgsn-servicesvc_name|username|username]+
```

<table>
<thead>
<tr>
<th>active-charging</th>
</tr>
</thead>
<tbody>
<tr>
<td>This feature is specific to the GGSN and is documented separately. See .</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>apn apn_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiates GTPP interim accounting for all PDP contexts accessing the specified APN. apn_name can be from 1 to 62, case sensitive, alphanumeric characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>calld call_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies a specific call. call_id must be followed by an 8-digit HEX number.</td>
</tr>
</tbody>
</table>

| cdr-types ( mcdr | scdr ) |
|-----------------|
| Specifies the CDR types to be generated by the SGSN: This keyword is specific to the SGSN. gcdr - Instructs the GGSN to only generate G-CDRs. mcdr - Instructs the SGSN to only generate M-CDRs scdr - Instructs the SGSN to only generate S-CDRs. |

<table>
<thead>
<tr>
<th>dhcp-server ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the DHCP server where the IP address (defined with the ip_address keyword) was allocated. Must be followed by the IP address of the DHCP server. ip_address: Must be specified using dotted decimal notation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ggsn-address ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>This keyword is specific to the GGSN. Specifies the IP address of the interface to the GGSN. ip_address: Must be specified using dotted decimal notation.</td>
</tr>
</tbody>
</table>
**ggsn-service svc_name**

This keyword is specific to the GGSN.
Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the specified GGSN service.
*svc_name* can be from 1 to 63, case sensitive, alphanumeric characters.

**gprs-service svc_name**

This keyword is specific to the SGSN.
Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the specified GPRS service.
This keyword is specific to the SGSN.
*svc_name* can be from 1 to 63, case sensitive, alphanumeric characters. Must be an already defined GPRS service name.

**imsi insi [ ip-address sub_address [ username name ] ] nsapi nsapi [ ip-address sub-address [ username name ] username name ]**

Initiates GTPP interim accounting for a specific International Mobile Subscriber Identity (IMSI) number. The request could be further filtered using any of the following keywords:

- **ip-address**: Interim accounting will be performed for the address specified by *sub_address*. The command can be further filtered by specifying a specific username (*name*) with that address.
- **nsapi**: Interim accounting will be performed for a specific Network Service Access Point Identifier (NSAPI). *nsapi* is an integer value from 5 to 15. The command can be further filtered by specifying a specific ip address (*sub_address*) and/or a username (*name*) with that address, or just a specific username.

**ip-address sub_address [ username name ]**

Initiates GTPP interim accounting for the address specified.
*sub_address* is the IP address of the subscriber and must be expressed in dotted decimal notation.
The command can be further filtered by specifying *username* with that address.
*name* is the subscriber’s name and can be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters in length. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘‘). For example: ‘$’.

**ip-pool pool_name**

This keyword is applicable to the GGSN only.
Initiates GTPP interim accounting for all PDP contexts that were allocated IP addresses from the specified pool.
*pool_name* can be from 1 to 31 alpha and/or numeric characters and is case sensitive.

**mcc mcc_number mnc mnc_number**

*mcc_number* Specifies the mobile country code (MCC) portion of the PLMN’s identifier and can be configured to any 3-digit integer value between 100 and 999.
*mnc_number* Specifies the mobile network code (MNC) portion of the PLMN’s identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.
**msisdn msisdn_num**

This keyword configures the SGSN to include the Mobile Subscribers Integrated Services Digital Network identifier in generated CDRs (M-CDRs and/or the S-CDRs).

This keyword is applicable for SGSN only.

*msisdn_number* - Must be followed by a valid MSISDN number, consisting of 1 to 15 digits.

**sgsn-address ip_address**

This keyword is specific to the GGSN.

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the specified SGSN.

*ip_address* is the IP address of the SGSN and must be expressed in dotted decimal notation.

**sgsn-service svc_name**

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the specified SGSN service.

This keyword is specific to the SGSN.

*svc_name* can be from 1 to 63, case sensitive, alphanumeric characters. Must be an already defined SGSN service name.

**username name**

Initiates GTPP interim accounting for all PDP contexts for the subscriber specified.

*name* is the subscriber’s name and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

+ 

More than one of the above keywords can be entered within a single command.

**Usage**

This command causes GTPP accounting CDRs to immediately be generated for all active sessions that are in the current context. If executed within the local context, CDRs will be generated for all active sessions regardless of context.

The sending of the CDRs is paced so as not to overload the accounting server.

**Example**

The following command causes CDRs to immediately be generated:

```
gtp p interim now
```
gtpp interim now active-charging egcdr

Check points current GTPP accounting messages for active charging immediately.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
gtpp interim now active-charging egcdr [ callid call_id | imsi imsi | msid msid | rulebase rbase_name | session-id sess_id | username name ]
```

- **callid call_id**
  Initiates GTPP interim accounting for a session with the specific call ID. `call_id` must be an 8-digit hexadecimal number.

- **imsi imsi**
  Initiates GTPP interim accounting for a specific International Mobile Subscriber Identity (IMSI) number. `imsi` must be a sequence of hexadecimal digits and wildcard characters - \$ matches a single character and \* matches multiple characters.

- **msid msid**
  Initiates GTPP interim accounting for a specific Mobile Station Identifier (MSID) number. `msid` must be a sequence of up to 24 digits and wildcard characters - \$ matches a single character and \* matches multiple characters.

- **rulebase rbase_name**
  Initiates GTPP interim accounting for sessions that use the named active charging rulebase. `rbase_name` must be an alpha and/or numeric string of from 1 through 24 characters.

- **session-id sess_id**
  Initiates GTPP interim accounting for a specific active charging session. `sess_id` must be the name of a current active charging session.

- **username name**
  Initiates GTPP interim accounting for all PDP contexts for the subscriber specified. `name` is the subscriber’s name and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Usage

This command causes GTPP accounting eG-CDRs to immediately be generated for active charging sessions that meet the specified criteria.
The sending of the CDRs is paced so as not to overload the accounting server.
Example
The following command causes eG-CDRs to immediately be generated for active charging sessions using the rulebase named rulebase1:

```
gtpp interim now active-charging egcdr rulebase rulebase1
```
gtpp storage-server commit

Causes the GTPP storage server to save all buffered packets to the hard drive.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
gtpp storage-server commit now
```

Usage

Upon execution, this command is relayed by the system to the GTPP Storage Server (GSS) causing the GSS to save all buffered packets to the hard drive. It also causes the GSS to delete all CDRs that have been acknowledged by the CGF. The deleted CDRs are saved in a separate file.

Note that this command must be executed from within the context in which the GSS is configured.

Refer to the `gtpp storage-server` command in the Context Configuration Mode for more information.
**gtpp test**

Tests the system’s ability to communicate with configured CGF(s).

**Product**

GGSN

**Privilege**

Operator, Config-Administrator, Administrator

**Syntax**

```
gtpp test [ accounting { all | cfg-server cfg_address } ] | [ storage-server { address ip-addr port udp-port } ]
```

*all*

Tests all CGFs configured within the given context.

*cfg-server
cfg_address*

Tests a specific CGF configured within the given context.

*ip_address* is the IP address of the CGF expressed in dotted decimal notation.

*storage-server [address ip-address port udp-port]*

Test the connectivity and provide round trip time for the echo request sent to GTPP Storage-Server configured in the requested context.

*ip_address* is the IP address of the GSS expressed in dotted decimal notation and *udp-port* is the port defined for GTPP Storage Server.

**Usage**

This command is used to verify the configuration of and test the system’s ability to communicate with one or all configured GSS/CGFs for monitoring or troubleshooting purposes. When executed, this command causes the system to send GTPP echo packets to the specified GSS/CGF(s). The command’s response will display whether the GSS/CGF is active or unreachable.

**Example**

The following command tests communication with a CGF having an IP address of 192.168.1.5:

```
gtpp test accounting cfg-server 192.168.1.5
```

The following command tests communication with a GSS configured in requested context

```
gtpp test storage-server
```

The following command verify communication with a GSS, having IP address 192.156.12.10 and port 50000, without configuring it in a context

```
gtpp test storage-server address 192.156.12.10 port 50000
```
gtpu test echo

Tests the ability of a GGSN service to exchange GTP-U echo request messages with the specified SGSN(s).

Product
GGSN

Privilege
Operator, Config-Administrator, Administrator

Syntax

gtpu test echo src-address gn_address { all | sgsn-address ip_address }

src-address gn_address
Specifies the IP address of a Gn interface configured on the system. 
gn_address must be expressed in dotted decimal notation.

Important: The IP address of the system’s Gn interface must be bound to a configured GGSN service prior to executing this command.

all
Specifies that GTP-U echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.

sgsn-address ip_address
Specifies that GTP-U echo requests will be sent to a specific SGSN. 
ip_address is the address of the SGSN to send the requests to and must be expressed in dotted decimal notation.

Usage
This command tests the GGSN’s ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring. 
This command must be executed from within the context in which the GGSN service is configured. 
Refer also to the gtpc test command.

Example
The following command issues GTP-U echo packets from a GGSN service bound to address 192.168.157.43 to an SGSN with an address of 192.168.1.52:

gtpu test echo src-address 192.168.157.43 sgsn-address 192.168.157.2

The following displays a sample of this command’s output.

GTPU test echo--------------SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 24 (COMPLETE)
gp filter test echo
gtpv0 test echo

Tests the ability of a GGSN service to exchange GTPv0 echo request messages with the specified SGSN(s).

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
gtpv0 test echo src-address gn_address { all | sgsn-address ip_address }
```

- **src-address gn_address**
  Specifies the IP address of a Gn interface configured on the system.
  `gn_address` must be expressed in dotted decimal notation.

- **all**
  Specifies that GTPv0 echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.

- **sgsn-address ip_address**
  Specifies that GTPv0 echo requests will be sent to a specific SGSN.
  `ip_address` is the address of the SGSN to send the requests to and must be expressed in dotted decimal notation.

Usage

This command tests the GGSN’s ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN service is configured.

Refer also to the gtpc test and gtpu test commands.

Example

The following command issues GTPv0 echo packets from a GGSN service bound to address 192.168.1.33 to an SGSN with an address of 192.168.1.42:

```
gtpv0 test echo src-address 192.168.1.33 sgsn-address 192.168.1.42
```

The following displays a sample of this command’s output.

```
GTPv0 test echo------------------SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 14
{COMPLETE) Recovery: 210 (0xD2)
```
gtpv0 test echo
**hd raid**

Performs the RAID management operations on the ASR 5000 hard drive.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
hd raid { check | { create { local1 | remotel } [ -force ] [ -noconfirm ] } | { overwrite { local1 | remotel } [ -force ] [ -noconfirm ] } | { select { local1 | remotel } [ -force ] [ -noconfirm ] } | { insert { local1 | remotel } [ -force ] [ -noconfirm ] } | { remove { local1 | remotel } [ -force ] [ -noconfirm ] }
```

**check**

Starts a background check on RAID disks unless the RAID is running in degraded mode. 

*noconfirm*: instructs system not to display “are you sure” prompts. 

*force*: instructs the system to enforce the action and override warnings.

**create local1 | remotel**

Overwrites the specified disk to create a new RAID that could run in degraded mode on the specified drive:

*local*: specifies the RAID is to be established on the primary SMC. 
*remote*: specifies the RAID is to be established on the backup SMC. 

*noconfirm*: instructs system not to display “are you sure” prompts. 

*force*: instructs the system to enforce the action and override warnings.

**overwrite local1 | remotel**

Overwrites the specified disk and adds it to the current running RAID to construct a fully mirrored array. 

*local*: specifies the primary SMC is to be added to the current RAID. 
*remote*: specifies the backup SMC is to be added to the current RAID. 

*noconfirm*: instructs system not to display “are you sure” prompts. 

*force*: instructs the system to enforce the action and override warnings.

**select local1 | remotel**

Selects the specified disk to assemble a RAID when two unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode. 

*local*: specifies the primary SMC is to assemble the RAID. 
*remote*: specifies the backup SMC is to assemble the RAID. 

*noconfirm*: instructs system not to display “are you sure” prompts. 

*force*: instructs the system to enforce the action and override warnings.

**insert local1 | remotel**

Inserts the specified disk to the running RAID causing it to recover from degraded mode. 

*local*: specifies the primary SMC is to be inserted into the RAID. 
*remote*: specifies the backup SMC is to be inserted into the RAID.
-noconfirm: instructs system not to display “are you sure” prompts. -force: instructs the system to enforce the action and override warnings.

remove local1 | remote1
Removes the specified disk from the running RAID causing it to run in degraded mode or to fail.
local1: specifies the primary SMC is to be removed from the RAID. remote1: specifies the backup SMC is to be removed from the RAID.
-noconfirm: instructs system not to display “are you sure” prompts. -force: instructs the system to enforce the action and override warnings.

Usage
All commands need confirmation unless the -noconfirm is included in the command. If the result will bring down a running RAID, you have to force the command using -force.
RAID commands are needed to intervene in the following situations:
- the hard disk controller task can not determine the correct operation,
- administrator action is required by policy
- the administrator wants to wipe out an unused disk.

In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.
To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These hd raid commands are described in the HD RAID Configuration Mode chapter of the Command Line Interface Reference.

Example
The following instructs the system to setup a RAID on the primary SMC hard drive.

```
hd raid create local1 -force
```
host

Used to resolve the IP address or logical host name information via DNS query.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
host { host_name | host_ip_address }
```

- `host_name | host_ip_address`
  - Specifies host for which IP information is to be displayed.
  - `host_name`: specifies the logical host name for which the IP address is to be displayed (via DNS lookup).
  - `host_ip_address`: specifies the IP address for which the associated logical host name(s) are to be displayed (via reverse DNS lookup).

Usage

Verify DNS information which affects connections and packet routing.

Example

The following will resolve the host information for `remoteABC` and `1.2.3.4`.

```
host remoteABCHost 1.2.3.4
```
interface sent gratuitous-arp

Use this command to configure the system to allow the manual generation of G-ARPs in case of a failure during inter-node online upgrade. If the chassis is not active, an error message displays.

Product
All

Privilege
Security Administrator, Administrator, Operator, or Inspector with li-administrator permissions

Syntax

```
interface name send gratuitous-arp ip-address
```

Usage
This command generates a G-ARP for the IP-ADDR specified and sends it out for the interface.

Example
The following generate a G-ARP for IP address 192.168.100.10.

```
interface interface_1 send gratuitous-arp 192.168.100.10
```
lawful-intercept

This command provisions/de-provisions the lawful interception of data for the specified subscriber session.

Product
PDSN, HA, LNS, GGSN, PDIF, SGSN, ASN-GW

Privilege
Security Administrator, or Administrator, Operator, or Inspector with li-administrator permissions

Syntax

```
lawful-intercept { [ imei imei_value ] [ imsi imsi_value ] [ ip-addr intercept_ip_addr ] [ msid ms_id ] [ msisdn msisdn_value ] [ username subscriber_name ] + } [ active-only ] [ allow-multiple-match ] [ calltype call_type ] [ intercept-id li_id ] [ li-context ctxt_name ] [ content-delivery { none | udp-unack-format-1 dest-addr df_ip_address dest-port df_port_no } event-delivery { none | udp-unack-format-1 | udp-ack-format-1 dest-addr df_ip_address dest-port df_port_no } ]
```

```
no lawful-intercept [ all ] { [ imei imei_value ] [ imsi imsi_value ] [ ip-addr intercept_ip_addr ] [ msid ms_id ] [ msisdn msisdn_value ] [ username subscriber_name ] + } [ calltype call_type ] [ content-delivery { none | udp-unack-format-1 dest-addr df_ip_address dest-port df_port_no } event-delivery { none | udp-ack-format | udp-unack-format } dest-addr ip_address dest-port port_no
```

- **no**
  De-provisions a previously configured lawful-intercept.

- **all**
  De-provisions all previously configured lawful-intercept warrant information. This Keyword is used to clear all warrant information in a single command `no lawful-intercept all`.

- **imei imei_value**
  Specifies the unique International Mobile Equipment Identifier (IMEI) which identifies the targeted device being used for a subscriber session to be intercepted.
  `imei_value` consists of 1 to 16 digits.

- **imsi imsi_value**
  Specifies the international mobile subscriber identity (IMSI) of the subscriber session to be intercepted.
  `imsi_value` is an integer value from 1 to 15 characters.

- **ip-addr intercept_ip_addr**
  Specifies the IP address assigned for the subscriber session or to the mobile station to be targeted for interception.
  `intercept_ip_addr` must be an IPv4/IPv6 address in desired notation.
**msid ms_id**
Specifies the mobile station identification (MSID) number, assigned by the home service provider, to be intercepted. 
*ms_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

**msisdn msisdn_value**
Specifies the unique mobile subscriber ISDN (telephone) number. 
*msisdn_value* consists of 1 to 15 digits.

**username subscriber_name**
Specifies the previously configured NAI username of the subscriber to be intercepted. 
*subscriber_name* is an alphanumeric string of 1 to 127 characters. 
Use of this keyword is not supported by the SGSN during LI provisioning or de-provisioning.

+ 
Indicates that multiple keywords can be specified in a single command entry. When the “+” appears in the syntax, any of the keywords that appear prior to the “+” can be entered in any order. 
This functionality is not supported by the SGSN during LI provisioning or de-provisioning.

**active-only**
Dictates that the interception applies only to calls currently in progress and not those that have not started. 
Use of this keyword is not supported by the SGSN during LI provisioning or de-provisioning.

**allow-multiple-match**
When used, interception is provided for up to 10 subscribers matching the specified criteria. This feature is disabled by default. 
Use of this keyword is not supported by the SGSN during LI provisioning.

**calltype call_type**
The type of call for the specified subscriber session. *call_type* must be one of the following:

- *asングw*
- *ммe*
- *pgw*
- *sgw*
- *gгssн*
- *pdif*
- *pdsn*
- *sgsn*
- *cссf*
- *ha*
- *lns*

Note that specifying call type is not mandatory while provisioning on SGSN and GGSN targets for any type of event and content delivery format.
content-delivery
Specifies the format in which the intercepted data content comprised of GTPU messages CC information is to be delivered to the DF.

event-delivery
Specifies the format in which intercepted control messages (such as attach/detach or RAU messages) IRI event messages are to be delivered to the DF.

intercept-id li_id
This is an arbitrary identification number, assigned by the provisioner, to identify this intercept definition. li_id must be an integer from 1 to 4294967295.

li-context ctxt_name
Identifies the destination context for intercepted packets. This keyword is mandatory if provisioning is done in a different context. ctxt_name must be an alpha/numeric string of 1 to 79 characters that specifies the name of an existing context.

none
Indicates that the intercepted data, specified as either delivery-type (content or event), is not to be sent to the DF. Entering none automatically activates the active-only provisioning method.

udp-unack-format-1
Dictates that the specified information type (content or event) is to be delivered using the udp-unack-format-1 which does not support acknowledgement messages for delivered information.

udp-ack-format-1
Dictates that the event information type is to be delivered using the udp-ack-format-1 which supports acknowledgement messages for delivered information.

dest-addr df_ip_address
The IP address of the DF to which the system sends intercepted data. df_ip_address must be an IPv4/IPv6 address in desired notation.

dest-port df_port_no
The port of the DF to which the system sends intercepted data. df_port_no can be any integer value from 1 to 65535.

Usage
Use this command to initiate a lawful Intercept of data for a subscriber. This command is not available to system accounts that do not have li-administrator privileges.
**Important:** You must log in to the system through a Secure Shell (SSH) using a system account that has administrator privileges to use this command. For details on using the Lawful Intercept capability of the system, refer to the System Administration and Configuration Guide.

**Example**

To lawfully intercept data from a subscriber session with an MSID of 0000100048, assign an intercept ID of 102, set the destination address to 192.168.100.10 and the destination port to 100, enter the following command:

```
lawful-intercept msid 0000100048 intercept-id 102 content-delivery udp-unack-format-1 dest-addr 192.168.100.10 dest-port 100 event-delivery none
```
lawful-intercept packet-cable

This command provisions/de-provisions the LI Call Content interception for PDSN or CSCF session.

Product
PDSN, SCM

Privilege
Security Administrator, or Administrator, Operator, or Inspector with li-administrator permissions

Syntax

lawful-intercept packet-cable {content-delivery {df-setup content id df_cont_id calltype {cscf | pdsn } dest-addr df_ip_address dest-port df_port_no li-context li_ctxt_name | intercept-request content id intercept_cont_id calltype {cscf | pdsn } filter-spec src-ip-addr src_ip_address} | event-delivery username subscriber_name intercept id intercept_id)

no lawful-intercept packet-cable {content-delivery content id df_cont_id calltype {cscf | pdsn } | event-delivery username subscriber_name calltype {cscf | pdsn}}

no
De-provisions a previously configured lawful-intercept.

**df-setup content id df_cont_id**
Specifies the DF setup and content identifier for subscriber to be intercepted.
df_cont_id must be an integer from 1 to 4294967295.

**intercept-request content id intercept_cont_id**
This is an arbitrary identification number, assigned by the provisioner, to identify this intercept definition.
intercept_cont_id must be an integer from 1 to 4294967295.

**calltype {cscf | pdsn}**
The type of call for the specified subscriber session.
pdsn: specifies the CDMA 2000 networks subscriber session.
cscf: specifies the SCM/IMS networks subscriber session.

**content-delivery**
Specifies the format in which the intercepted data content is to be delivered to the DF.

**event-delivery**
Specifies the format in which intercepted control messages IRI event messages are to be delivered to the DF.

**username subscriber_name**
Specifies the previously configured NAI username of the subscriber to be intercepted.
subscriber_name is an alphanumeric string of 1 to 127 characters.
**li-context li_ctx_name**

Identifies the destination context for intercepted packets. This keyword is mandatory if provisioning is done in a different context. `li_ctx_name` must be an alpha/numeric string of 1 to 79 characters that specifies the name of an existing context.

**dest-addr df_ip_address**

The IP address of the DF to which the system sends intercepted data. `df_ip_address` must be an IPv4/IPv6 address in desired notation.

**dest-port df_port_no**

The port of the DF to which the system sends intercepted data. `df_port_no` can be any integer value from 1 to 65535.

**filter-spec src-ip-addr src_ip_address**

The IP address of the source filter from which the system retrieves intercepted data. `src_ip_address` must be an IPv4/IPv6 address in desired notation.

**Usage**

Use this command to initiate a packet-cable lawful Intercept for a PDSN or CSCF subscriber. This command is not available to system accounts that do not have li-administrator privileges.

**Important:** You must log in to the system through a Secure Shell (SSH) using a system account that has li-administrator privileges to use this command. For details on using the Lawful Intercept capability of the system, refer to the System Administration and Configuration Guide.

**Example**

Following command enables the LI Call Content interception for CSCF with DF setup having content id 10203 with destination address 1.2.3.4, port 2300 and LI context `li_cscf1`:

```
lawful-intercept packet-cable content-delivery df-setup content id 10203
calltype cscf dest-addr 1.2.3.4 dest-port 2300 li-context li_cscf1
```
lawful-intercept ssdf

This command is used to configure and provision the SSDF generic interface for LI Call Content interception during CSCF session in IMS network.

**Product**
SCM

**Privilege**
Security Administrator, or Administrator, Operator, or Inspector with li-administrator permissions

**Syntax**

```
lawful-intercept ssdf dest-addr df_ip_address dest-port df_port_no serial-number sr_num version vr_num [li-context li_ctxt_name]

[no] lawful-intercept ssdf [li-context li_ctxt_name] dest-addr df_ip_address dest-port df_port_no
```

- **no**
  De-provisions a previously configured lawful-intercept.

- **dest-addr df_ip_address**
  The IP address of the DF to which the system sends intercepted data. `df_ip_address` must be an IPv4/IPv6 address in desired notation.

- **dest-port df_port_no**
  The port of the DF to which the system sends intercepted data. `df_port_no` can be any integer value from 1 to 65535.

- **li-context li_ctxt_name**
  Identifies the destination context for intercepted packets. This keyword is mandatory if provisioning is done in a different context. `li_ctxt_name` must be an alpha/numeric string of 1 to 79 characters that specifies the name of an existing context.

- **serial-number sr_num**
  Identifies the Serial Number of the Access Function (AF) for validation which is to be provisioned on SSDF interface. `sr_num` must be an ASCII string of 1 to 79 characters that represents the serial number of the access function equipment.

- **version sr_num**
  Identifies the software version of the software running on the Access Function (AF) for validation which is to be provisioned on SSDF interface. `sr_num` must be an ASCII string of 1 to 79 characters that represents the software version running on the access function equipment.
Usage

Use this command to configure/provision the SSDF generic interface for lawful Intercept on a CSCF function. This command is not available to system accounts that do not have li-administrator privileges.

Important: You must log in to the system through a Secure Shell (SSH) using a system account that has li-administrator privileges to use this command. For details on using the Lawful Intercept capability of the system, refer to the System Administration and Configuration Guide.

Example

Following command configures the SSDF interface with AF number 10203 software version 2 with destination address 1.2.3.4, port 2300 and LI context li_cscfl:

```
    lawful-intercept ssdf dest-address 1.2.3.4 dest-port 2300 serial-number 10203 version 2 li-context li_cscfl
```
logging active

Enables/disables logging for active internal log files.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
logging active [ copy runtime filters ] [ event-verbosity event_level] [ pdu-data format ] [ pdu-verbosity pdu_level ]
```

```plaintext
no logging active
```

**no**
Indicates the internal logging is to be disabled.

**copy runtime filters**
When this command is issued, it makes a copy of the runtime filters and makes that copy the filters for the current logging session.

**event-verbosity event_level**
Specifies the level of verboseness to use in logging of events as one of:
- **min** - displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- **concise** - displays detailed information about the event, but does not provide the event source within the system.
- **full** - displays detailed information about event, including source information, identifying where within the system the event was generated.

**pdu-data format**
Specifies output format for packet data units when logged as one of:
- **none** - output is in raw format (unformatted).
- **hex** - output being displayed in hexadecimal format.
- **hex-ascii** - output being displayed in hexadecimal and ASCII similar to a main-frame dump.

**pdu-verbosity pdu_level**
Specifies the level of verboseness to use in logging of packet data units as a value from 1 to 5 where 5 is the most detailed.

**Usage**
Adjust the active logging levels when excessive log file sizes are being generated or, conversely, not enough information is being sent to the active log files for adequate troubleshooting support. The no keyword is used to disable internal logging.

**Important:** A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

**Important:** Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

**Example**
The following sets the active logging for events to the maximum.

```plaintext
logging active event-verbosity full
```

The following command sets the active logging for packet data units to level 3 and sets the output format to the main-frame style hex-ascii.

```plaintext
logging active pdu-data hex-ascii pdu-verbosity 3
```

The following disables internal logging.

```plaintext
no logging active
```
logging filter

Sets the logging filtering options for all or individual facilities.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
logging filter active facility facility level severity_level [ critical-info | no-critical-info ]
```

- **active**
  Indicates only active processes are to have logging options set.

- **facility**
  Specifies the facility to modify the filtering of logged information for as one of:

  - **a10**: A10 interface facility
  - **a11**: A11 interface facility
  - **a11mgr**: A11 Manager facility
  - **aaa-client**: AAA client facility
  - **aaamgr**: AAA manager logging facility
  - **aaaproxy**: AAA Proxy facility
  - **acl-log**: Access Control List logging facility
  - **acsctrl**: Active Charging Service (ACS) Controller facility
  - **acsmgr**: Active Charging Service (ACS) Manager facility
  - **alarmctrl**: Alarm Controller facility
  - **all**: All facilities
  - **asf**: Voice Application Server Framework logging facility
  - **asfprt**: ASF Protocol Task (SIP) logging facility
  - **asngwmgr**: ASN Gateway Manager facility
  - **asnlrmgr**: ASN Paging/Location-Registry Manager facility
  - **bgp**: Border Gateway Protocol (BGP) facility
  - **cli**: CLI logging facility
  - **cscf**: IMS/MMD CSCF
  - **cscfmgr**: SIP CSCF Manager facility
  - **csp**: Card Slot Port controller facility
  - **css**: Content Service Selection (CSS) facility
  - **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
<table>
<thead>
<tr>
<th>Facility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcardctrl</td>
<td>IPSEC Daughtercard Controller logging facility</td>
</tr>
<tr>
<td>dcardmgr</td>
<td>IPSEC Daughtercard Manager logging facility</td>
</tr>
<tr>
<td>dhcp</td>
<td>DHCP facility (GGSN product only)</td>
</tr>
<tr>
<td>dhost</td>
<td>Distributed Host logging facility</td>
</tr>
<tr>
<td>diameter</td>
<td>Diameter endpoint logging facility</td>
</tr>
<tr>
<td>diameter-acct</td>
<td>Diameter Accounting</td>
</tr>
<tr>
<td>diameter-auth</td>
<td>Diameter Authentication</td>
</tr>
<tr>
<td>diameter-ecs</td>
<td>ECS Diameter signaling facility</td>
</tr>
<tr>
<td>diameter-svc</td>
<td>Diameter Service</td>
</tr>
<tr>
<td>diamproxy</td>
<td>DiamProxy logging facility</td>
</tr>
<tr>
<td>dpath</td>
<td>IPSEC Data Path facility</td>
</tr>
<tr>
<td>drvctrl</td>
<td>Driver Controller facility</td>
</tr>
<tr>
<td>egtpc</td>
<td>eGTP-C logging facility</td>
</tr>
<tr>
<td>egtpmgr</td>
<td>eGTP manager logging facility</td>
</tr>
<tr>
<td>egtpu</td>
<td>eGTP-U logging facility</td>
</tr>
<tr>
<td>evlog</td>
<td>Event log facility</td>
</tr>
<tr>
<td>famgr</td>
<td>Foreign Agent manager logging facility</td>
</tr>
<tr>
<td>firewall</td>
<td>Firewall logging facility</td>
</tr>
<tr>
<td>gss-gcdr</td>
<td>GTTP Storage Server GCDR facility</td>
</tr>
<tr>
<td>gtpc</td>
<td>GTP-C protocol logging facility (GGSN product only)</td>
</tr>
<tr>
<td>gtpcmgr</td>
<td>GTP-C protocol Manager logging facility (GGSN product only)</td>
</tr>
<tr>
<td>gtpp</td>
<td>GTP-PRIME protocol logging facility (GGSN product only)</td>
</tr>
<tr>
<td>gtpu</td>
<td>GTP-U protocol logging facility (GGSN product only)</td>
</tr>
<tr>
<td>h248prt</td>
<td>H.248 Protocol logging facility</td>
</tr>
<tr>
<td>hamgr</td>
<td>Home Agent manager logging facility</td>
</tr>
<tr>
<td>hat</td>
<td>High Availability Task (HAT) process facility</td>
</tr>
<tr>
<td>ims-authorizatn</td>
<td>IMS Authorization Service facility</td>
</tr>
<tr>
<td>ip-arp</td>
<td>IP Address Resolution Protocol facility</td>
</tr>
<tr>
<td>ip-interface</td>
<td>IP interface facility</td>
</tr>
<tr>
<td>ip-route</td>
<td>IP route facility</td>
</tr>
<tr>
<td>ipsec</td>
<td>IP Security logging facility</td>
</tr>
<tr>
<td>ipsgmgr</td>
<td>IP Services Gateway facility</td>
</tr>
<tr>
<td>ipsp</td>
<td>IP Pool Sharing Protocol logging facility</td>
</tr>
<tr>
<td>l2tp-control</td>
<td>L2TP control logging facility</td>
</tr>
<tr>
<td>l2tp-data</td>
<td>L2TP data logging facility</td>
</tr>
<tr>
<td>l2tpdemux</td>
<td>L2TP Demux Manager logging facility</td>
</tr>
<tr>
<td>l2tpmgr</td>
<td>L2TP Manager logging facility</td>
</tr>
</tbody>
</table>
• li: Lawful intercept facility (Logs are visible only to system accounts with li-administrator privileges.)
• magmgr: Mobile Access Gateway manager logging facility
• mme-app: Mobility Management Entity Application logging facility
• mmedemux: Mobility Management Entity Demux Manager logging facility
• mme-hss: Mobility Management Entity logging facility
• mme-misc: Mobility Management Entity Miscellaneous logging facility
• mobile-ip: Mobile IP processes
• mobile-ip-data: Mobile IP data facility
• mobile-ipv6: Mobile IPv6 logging facility
• multicast-proxy: Multicast Proxy logging facility
• nas: Network Access Signaling logging facility
• netwstrg: Network Storage facility
• npuctrl: Network Processor Unit Control facility
• npumgr: Network Processor Unit Manager facility
• nsctrl: Charging Service Controller facility (supported in conjunction with ECSv1)
• nsmgr: Charging Service Manager facility
• nsproc: Charging Service process facility
• orbs: Object Request Broker System logging facility
• ospf: OSPF logging facility
• pdg: PDG logging facility
• pgw: PDN Gateway logging facility
• ppp: PPP link and packet facilities
• radius-acct: RADIUS accounting logging facility
• radius-auth: RADIUS authentication logging facility
• radius-coa: RADIUS change of authorization and radius disconnect
• rct: Recovery Control Task logging facility
• rdt: Redirect Task logging facility
• resmgr: Resource Manager logging facility
• rip: RIP logging facility (RIP is not supported at this time.)
• rohc: RObust Header Compression facility
• rsvp: Reservation Protocol logging facility
• scct: Shared Configuration Task logging facility
• sessctrl: Session Controller logging facility
• sessmgr: Session Manager logging facility
• sft: Switch Fabric Task logging facility
• sgw: Serving Gateway logging facility
• sipcdprt: Sip Call Distributor facility
logging filter

- **sitmain**: System Initialization Task main logging facility
- **snmp**: SNMP logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **ssh-ipsecc**: SSH IP Security logging facility  
  - **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **threshold**: threshold logging facility
- **ttg**: TTG logging facility
- **udr**: User detail record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6

**level severity_level**

Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- **critical**: display critical events
- **error**: display error events and all events with a higher severity level
- **warning**: display warning events and all events with a higher severity level
- **unusual**: display unusual events and all events with a higher severity level
- **info**: display info events and all events with a higher severity level
- **trace**: display trace events and all events with a higher severity level
- **debug**: display all events

**critical-info | no-critical-info**

Default: critical-info enabled.

- **critical-info**: specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated.
- **no-critical-info**: specifies that events with a category attribute of critical information are not to be displayed.

**Usage**

Apply filters for logged data to collect only that data which is of interest.
**Important:** A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

**Important:** Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

**Caution:** Issuing this command could negatively impact system performance depending on the amount of system activity at the time of execution and/or the type of facility(ies) being logged.

**Example**
The following are selected examples used to illustrate the various options. Not all facilities will be explicitly shown as each follows the same syntax for options.
The following sets the level to log only warning information for all facilities.

```
logging filter active facility all level warning
```

The following enables the logging of critical information for the SNMP facility while setting the level to error.

```
logging filter active facility snmp level error critical-info
```
logging trace

Enables/disables the logging of trace information for specific calls, mobiles, or network addresses.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

logging trace { callid call_id | ipaddr ip_address | msid ms_id | username user_name }

no logging trace { callid call_id | ipaddr ip_address | msid ms_id | username user_name }

no
Indicates the logging of trace information is to be disabled.

callid call_id | ipaddr ip_address | msid ms_id | username user_name

callid call_id: specifies the exact call instance ID which is to have trace data logged. call_id is specified as a 4-byte hexadecimal number.
ipaddr ip_address: specifies the IP address for which trace information is to be logged. ip_address must be specified using the standard IPv4 dotted decimal notation.
msid ms_id: specifies the mobile subscriber ID for which trace information is to be logged. ms_id must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.
username user_name: specifies a user who is to have trace information logged. user_name must refer to a previously configured user.

Usage

A trace log is useful in troubleshooting subscriber problems as well as for system verification by using a test subscriber. The no keyword is used to stop the logging of trace information.

Important: A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important: Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Caution: Issuing this command could negatively impact system performance depending on the number of subscribers connected and the amount of data being passed.
**Example**
The following commands enables/disables trace information for user user1.

```
logging trace username user1
no logging trace username user1
```

The following commands will enable/disable trace information logging for the user assigned IP address 1.2.3.4.

```
logging trace ipaddr 1.2.3.4
no logging trace ipaddr 1.2.3.4
```

The following enables/disables logging of trace information for call ID FE80A12.

```
logging trace callid fe80a12
no logging trace callid fe80a12
```
logs checkpoint

Performs check pointing operations on log data. Check pointing identifies logged data as previously viewed or marked. Check pointing results in log information since the last check point being displayed only, i.e., check pointed log data is not available for viewing.

Individual logs may have up to 50,000 events in the active log. Check pointing the logs will then result in at most 50,000 events being in the inactive log files. This gives a maximum of 100,000 events in total which are available for each facility logged.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
logs checkpoint
```

**Usage**
Check point log data to a set the log contents to a well know point prior to special activities taking place. This command may also be a part of periodic regular maintenance to manage log data. The check pointing of logs moves the current log data to the inactive logs. Only the most recently check pointed data is retained in the inactive logs. A subsequent check pointing of the logs will result in the prior check pointed inactive log data being cleared and replaced with the newly check pointed data. The check pointing of log data moves the active log data to be retained as the inactive log data. This results in the active log data, if displayed, having no data earlier than the point in time when the check pointing occurred.

**Important:** Check pointing of logs should be done periodically to avoid the logs becoming full. Logs which have 50,000 events logged will discard the oldest events first when new events are to be logged.

**Example**

```
logs checkpoint
```
mkdir

Creates a new directory in the local file system or in remote locations as specified.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
mkdir filepath
```

`filepath`
Specifies the directory path to create. The path must be formatted as follows:
Specifies the source of the copy. `url` may refer to a local or a remote file. `url` must be entered using one of the following formats:
- ASR 5000:

  ```bash
  [file:][/flash|/pcmcia|/hd][/directory]/file_name
  ```

**Important:** Use of the SMC hard drive is not supported in this release.

`directory` is the directory name
`filename` is the actual file of interest

Usage
Create new directories as part of periodic maintenance activities to better organize stored files.

Example
The following creates the directory `/flash/pub` in the local flash storage.

```bash
mkdir /flash/pub
```
monitor protocol

Enters the system’s protocol monitoring utility.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```plaintext
monitor protocol
```

**Usage**

Useful for troubleshooting, this command provides a tool for monitoring protocol transactions between the system and other network nodes including the mobile station(s).

The following protocols can be monitored:

- SNMP
- RADIUS Authentication
- RADIUS Accounting
- A11 (R-P Interface) (PDSN only)
- Mobile IPv4
- A11MGR
- PPP
- A10 (PDSN only)
- User L3 (User Layer 3 protocols)
- L2TP
- L2TPMGR
- L2TP Data
- GTPC
- GTPCMGR
- GTPU
- GTPP
- DHCP (GGSN only)
- CDR
- DHCPV6
- RADIUS COA
- MIP Tunnel
- L3 Tunnel (Layer 3 Tunnel Protocols)
- CSS Data
- CSS Signaling

- EC Diameter (Diameter Enhanced Charging)
- SIP
- IPSec IKE Inter-Node
- IPSec IKE Subscriber
- IPSG RADIUS Signal
- ROHC (Robust Header Compression) (PDSN only)
- WiMAX R6
- WiMAX Data
- SRP
- BCMCS SERV AUTH
- RSVP
- Mobile IPv6
- ASNGWMGR
- ASNPCMGR
- STUN
- SCTP
- M3UA
- SCCP
- TCAP
- MAP
- RANAP
- GMM
- GPRS-NS
- BSSGP
- CAP
- SSCOP
- SSCFNNI
- MTP3
- LLC
- SNDCP
- BSSAP+
- SMS
- PHS-Control
- PHS-Data
DNS Client
HNBP: Enabling this option will display the HNB Application Part (HNBP) protocol packets.
RUA: Enabling this option will display the RANAP User Adaptation (RUA) protocol packets.
MTP2
EGTPC
App Specific Diameter
PHS-EAPOL
ICAP
Micro-Tunnel
ALCAP
SSL
S1-AP
NAS

Once the protocol has been selected, the utility monitors and displays every relative protocol message transaction. Protocol monitoring is performed on a context-by-context-basis. Therefore, the messages displayed are only those that are transmitted/received within the system context from which the utility was executed.

**Caution:** Protocol monitoring can be intrusive to subscriber sessions and could impact system performance. Therefore, it should only be used as a troubleshooting tool.

**Example**
The following command opens the protocol monitoring utility:

`monitor protocol`

The following displays a sample of this command's output with verbosity level 2 for GTPC:

```plaintext
*** Verbosity Level ( 2) ***INBOUND>>>> 04:39:58:808 Eventid:47000(3)GTPC Rx PDU, from 192.168.35.3:2123 to 192.168.35.1:2123 (190)TEID: 0x00000000, Message type: GTP_CREATE_PDP_CTX_REQ_MSG (0x10)INFORMATION ELEMENTS FOLLOW: IMSI: 40427000000001ROUTING AREA IDENTITY (RAI) FOLLOWS: MCC: 333 MNC: 444 LAC:0 RAC:0ROUTING AREA IDENTITY (RAI) ENDS: Recovery: 0x01 (1) Selection Mode: 0x1 (MS provided APN, subscription not verified (Sent by MS)) Tunnel ID Data I: 0x000000400 Tunnel ID Control I: 0x000000400 NSAPI: 0x05 (5) Charging Characteristics: 0x0800 (Normal) End User Address: Organisation=IETF, PDP Type=IPv4, Address=10.0.0.1 Access Point Name: starent.comPROTOCOL CONFIG. OPTIONS FOLLOW: Protocol id: 0xC021 (LCP) Protocol length: 0x0E (14) Protocol contents: 0103000E0506D38509B0304C023 Protocol id: 0xC021 (LCP) Protocol length: 0x0E (14) Protocol contents: 0203000E0506D38509B0304C023 Protocol id: 0xC023 (PAP) Protocol length: 0x12 (18) Protocol contents: 0104001208E626E73757365720461626364PROTOCOL CONFIG. OPTIONS END. GSN Address I: 0xC0A82303 (192.168.35.3) GSN Address II: 0xC0A82303 (192.168.35.3) MSISDN: 9876543210 QOS Profile: 0x0122720D739640886074048 USER LOCATION INFORMATION: 111-22-3333-44444 IMEI(SV): 88888888866666622INFORMATION ELEMENTS END.
```
The following displays a sample of this command's output with verbosity level 3 for the Session Initiation Protocol (SIP):

**monitor subscriber**

Enables the system’s subscriber monitoring utility.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
monitor subscriber [ asn-peer-address bs_peer_address | callid call_id | imsi imsi_value | ipaddr ip_address | ipv6addr ipv6_address | ipsg-peer-address ipsg_peer_address | msid ms_id | msisdn msisdn | next-call | pcf pcf_address | pdif-peer-address pdif_peer_address | peer-fa peer_fa_address | peer-lac lac_peer_address | sgsn-address sgsn_address | type { 1xrtt | asngw | asnpc | closedrp | evdorev0 | evdoreva | interrogating-cscf | ggsn [ Next-Call By APN ] | ha | ipsg | lns | mme | pdif | proxy-cscf | rfc3261-proxy | serving-cscf | next-call | type bcmcs { next-call | next-service-request } | username user_name | Next-Call By APN ]
```

**asn-peer-address bs_peer_address**
Specifies the peer ASN Base Station IP address. Must be followed by IPv4 address in dotted decimal notation.

**callid call_id**
Specifies the call identification number assigned to the subscriber session by the system to be monitored. 
*call_id* is specified as a 4-byte hexadecimal number.

**imsi imsi_value**
Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored. 
*imsi_value* is an integer value from 1 to 15 characters.

**ipaddr ip_address**
Specifies the IP address of the subscriber session to be monitored. 
*ip_address* must be specified using dotted decimal notation.

**ipv6addr ipv6_address**
Specifies the IPv6 address of the subscriber session to be monitored. 
*ipv6_address* must be an IPv6 IP address entered using colon (:) separated notation.

**ipsg-peer-address ipsg_peer_address**
Specifies the peer IPSG IP address. Must be followed by IPv4 address in dotted decimal notation.

**msid ms_id**
Specifies the mobile subscriber identification number to be monitored.
ms_id\text{m}ust be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

\text{msisdn} \text{msisdn}

Specifies the Mobile Subscriber ISDN number to be monitored.
\text{msisdn} must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

\text{next-call}

Specifies that the system will monitor the next incoming subscriber session.

\text{pcf} \text{pcf\_address}

Specifies the PCF IP address. Must be followed by IPv4 address in dotted decimal notation.

\text{pdif-peer-address} \text{pdif\_peer\_address}

Specifies the peer PDIF IP address. Must be followed by IPv4 address in dotted decimal notation.

\text{peer-fa} \text{peer\_fa\_address}

Specifies the peer FA IP address. Must be followed by IPv4 address in dotted decimal notation.

\text{peer-lac} \text{lac\_peer\_address}

Specifies the peer LAC IP address. Must be followed by IPv4 address in dotted decimal notation.

\text{sgsn-address} \text{sgsn\_address}

Specifies the SGSN IP address. Must be followed by IPv4 address in dotted decimal notation.

\text{type} \{ \text{1xrtt} | \text{asngw} | \text{asnpo} | \text{evdorev0} | \text{evdoreva} | \text{interrogating-cscf} | \text{ggsn} [ \text{Next-Call By APN} ] | \text{ha} | \text{ipsg} | \text{lns} | \text{mme} | \text{openrp} | | \text{pdif} | | \text{proxy-cscf} | \text{rfc3261-proxy} | \text{serving-cscf} \} \text{next-call}

Allows monitoring for specific subscriber types established in the system when next call occurs.

- \text{1xrtt}: Displays logs for cdma2000 1xRTT call session subscriber
- \text{asngw}: Displays logs for ASN GW call session subscriber
- \text{asnpo}: Displays logs for ASN PC/LR call session subscriber
- \text{evdorev0}: Displays logs for cdma2000 EVDO Rev0 call session subscriber
- \text{evdoreva}: Displays logs for cdma2000 EVDO RevA call session subscriber
- \text{interrogating-cscf}: Displays logs for Interrogating CSCF subscriber
- \text{ggsn}: Displays logs for UMTS GGSN call session subscriber
- \text{Next-Call By APN}: Display logs for next call on APN basis, where APN name can be any of Gi or Gn
- \text{apn}.
- \text{ha}: Displays logs for Home Agent call session subscriber
- \text{ipsg}: Displays logs for IPSG call session subscriber
- \text{lns}: Displays logs for LNS call session subscriber
- \text{mme}: Displays logs for MME session subscribers.
- \text{openrp}: Displays logs for OpenRP subscriber
• **pdif**: Displays logs for PDIF call session subscriber
• **proxy-cscf**: Displays logs for Proxy CSCF subscriber
• **rfc3261-proxy-cscf**: Displays logs for non-ims-proxy (RFC-3261 proxy) subscriber
• **serving-cscf**: Displays logs for Serving CSCF subscriber

```plaintext
type bcmcs {next-call / next-service-request}
```
Specifies the type of BCMCS call for the subscriber.

```plaintext
username user_name
```
Specifies the username of the subscriber to be monitored. `user_name` refers to a previously configured user.

**Usage**
The monitor subscriber utility provides a useful tool for monitoring information about and the activity of either a single subscriber or all subscribers with active sessions within a given context. The following items can be monitored:

- Control events
- Data events
- Event ID information
- Inbound events
- Outbound events
- Protocols (identical to those monitored by `command` command)

Once the criteria has been selected, the utility will monitor and display every relative piece of information on the subscriber(s).

**Important:** Option Y for performing multi-call traces is only supported for use with the GGSN. This option is available when monitoring is performed using the “Next-Call” option. It allows you to monitor up to 11 primary PDP contexts for a single subscriber.

Subscriber monitoring is performed on a context-by-context-basis. Therefore, the information displayed will be only that which is collected within the system context from which the utility was executed.

**Caution:** Subscriber monitoring can be intrusive to subscriber sessions and could impact system performance. Therefore, it should only be used as a troubleshooting tool.

**Example**
The following command enables monitoring for user `user1`.

```plaintext
monitor subscriber username user1
```

The following command will enable monitoring for the user assigned IP address `1.2.3.4`.

```plaintext
monitor subscriber ip-address 1.2.3.4
```
The following enables monitoring for call ID FE80AA12.

```
monitor subscriber callid fe80aa12
```
newcall policy

Configures new call policies for busy-out conditions.

**Product**

PDSN, GGSN, MME, HA, LNS, P-CSCF, ASN GW, ASN PC/LR

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
newcall policy {asngw-service asnpc-service} {all | name service_name} reject
newcall policy cscc-service { all | nameservice_name } { 
redirect target_ip_address [ weight weight_num ] [ target_ipaddress2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ] | reject }
newcall policy { fa-service | lns-service | mipv6ha-service } { all | name service_name } reject
newcall policy { ha-service | pdns-service} { all | name service_name } { 
redirect target_ip_address [ weight weight_num ] [ target_ipaddress2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ] | reject }
newcall policy ggsn-service { apn_name apn_name | all | name ggsn-service-name } reject
no newcall policy { fa-service | ggsn-service | ha-service | mipv6ha-service | pdns-service| lns-service } { all | name service_name }
newcall policy mme-service {all | nameservice_name } reject
nonewcallpolicy { ha-service | pdns-service } { all | nameservice_name }
redirect target_ip_address [ weight weight_num ] [ target_ip_address2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ] }
no newcall policy ggsn-service { apn_name apn_name | all | name ggsn-service-name } reject
no newcall policy { asngw-service | asnpc-service } { all | name service_name }
no newcall policy mme-service { all | name service_name}
```

**no**

Disables the new call policy for all or specified service of a service type.

```
newcall policy { asngw-service | asnpc-service } { all | name service_name } reject
```

Creates a new call policy to reject the calls based on the specified ASN GW or ASN PC/LR service name or all services of this type.

**asngw-service**: Specifies the type of service as ASN GW for which new call policy is configured.
Exec Modes Commands (D-S)

newcall policy { cscf-service | fa-service | lns-service | mipv6ha-service } { all | name service_name } reject

Creates a new call policy that rejects calls based on the specified access point name.

no newcall policy { cscf-service | fa-service | ggsn-service | ha-service | mipv6ha-service | pdsn-service } { all | name service_name }

Removes a previously configured new call policy for the specified service.

no newcall policy { ha-service | pdsn-service } { all | name service_name } redirect target_ip_address [ weight weight_num ] [ target_ip_address2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ] }

Deletes up to 16 IP addresses from the redirect policy. The IP addresses must be expressed in IP v4 dotted decimal notation.

cscf-service | fa-service | ggsn-service | ha-service | lns-service | mipv6ha-service | pdsn-service }

Specifies the type of service for which to configure a new call policy. The following services are supported:

- **cscf-service**: A Call/Session Control Function service
- **fa-service**: A Foreign Agent service
- **ggsn-service**: A Gateway GPRS Support Node service
- **ha-service**: A Home Agent service
- **lns-service**: An L2TP Network Server service
- **mipv6ha-service**: A Mobile IPv6 Home Agent service
- **pdsn-service**: A Packet Data Serving Node service

{ all | name service_name }

Specifies a filter for the new call policy. Whether the new call policy will be applied to all configured services or a specific one.

- **all**: Specifies that the new call policy will be applied to all instances of the selected service type.
- **name service_name**: Specifies the name of a specific instance of the selected service type. service_name can be between 1 and 63 alpha and/or numeric characters and is case sensitive.

redirect target_ip_address [ weight weight_num ] [ target_ip_address2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ] }

Configures the busy-out action. When a redirect policy is invoked, the service rejects new sessions and provides the IP address of an alternate destination. This command can be issued multiple times.

address: The IP address of an alternate destination expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you
try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

**weight weight_num** When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. **weight_num** must be an integer from 1 through 10.

Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply:

- **ha service**: 88H (Registration Denied - unknown home agent address)
- **pdsn service**: 88H (Registration Denied - unknown PDSN address)

**Important**: The redirect option is not supported for use with FA and GGSN services.

```
newcall policy mme-service) {all | name service_name} reject
```

Creates a new call policy to reject the calls based on the specified MME service name or all MME services on the system.

- **name service_name**: Specifies the name of the MME service for which new call policy is configured.
- **service_name**: is name of a configured MME service.
- **reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For MME service rejection code is 81H (Registration Denied - administratively prohibited).

**reject**

Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply to indicate the rejection:

- **asngw service**: 81H (Registration Denied - administratively prohibited)
- **fa service**: 41H (administratively prohibited)

**Important**: When the newcall policy is set to reject for the FA service, the Busy Bit is set in the Agent Advertisement. Any further RRQs will be rejected with this code value.

- **ggsn service**: C7H (Rejected - no resources available)
- **ha service**: 81H (Registration Denied - administratively prohibited)
- **mipv6ha-service**: 81H (Registration Denied - administratively prohibited)
- **mme service**: 81H (Registration Denied - administratively prohibited)
- **pdsn service**: 81H (Registration Denied - administratively prohibited)

**Usage**

This command is used to busy-out specific system services prior to planned maintenance or for troubleshooting.

**Example**

The following command creates a new call policy to re-direct all new calls for all PDSN services to a device having an IP address of 192.168.1.23:
newcall policy psdn-service all redirect 192.168.1.23

The following command creates a new call policy to reject all new calls for a GGSN service called ggsn1:

newcall policy ggsn-service name ggsn1 reject

The following command creates a new call policy to reject all new calls for an MME service called MME1:

newcall policy mme-service name MME1 reject
password change

Provides a mechanism for local-user administrative users to change their passwords.

Product
All

Privilege
All local-user administrative levels except as noted below

Syntax

```
password change [ local-user name ]
```

- **local-user name**
  Specifies the name of the local-user administrative user for which to change the password.
  name can be from 3 to 16 alpha and/or numeric characters in length and is case sensitive.

**Important:** This keyword is only available to local-users with an authorization level of security-administrator.

Usage
This command provides a mechanism for local-user administrative users to change their passwords. In addition, it also provides a mechanism for security-administrator local-users to change the password for other local-user accounts.

If the local-user keyword is not entered, the system prompts the user for their current password and for the new password. New passwords take effect at the next login. Users that have had their password changed by a security-administrator are prompted to change their passwords at their next login.

New passwords must meet the criteria dictated by the local-user password command options in the Global Configuration Mode.

**Important:** The system does not allow the changing of passwords unless the time limit specified by the local-user passwordmin-change-interval has been reached.

Example
The following command, executed by a security-administrator, resets the password for a local-user name operator12:

```
password change local-user operator12
```
ping

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Important: Inspector privileges are granted for all variables except count. To initiate a ping count, you must have a minimum privilege level of Operator.

Syntax

```
ping host_ip_address [ broadcast ] [ count num_packets ] [ pattern packet_pattern ] [ size octet_count ] [ src { src_host_name | src_host_ip_address } ] [ | { grep grep_options | more } ]
```

**host_ip_address**
Identifies the remote node to which the ability to communicate with is to be verified.

**broadcast**
Sends ping packets to broadcast addresses.

**count num_packets**
Default: 5
Specifies the number of packets to send to the remote host for verification. num_packets must be within the range 1 through 10000.

**pattern packet_pattern**
Default: each octet of the packet is encoded with the octet number of the packet.
Specifies a pattern to use to fill the internet control message protocol packets with. packet_pattern must be specified in hexadecimal format with a value in the range hexadecimal 0x0000 through 0xFFFF. packet_pattern must begin with a ‘0x’ followed by up to 4 hexadecimal digits.

**size octet_count**
Default: 56
Specifies the number of bytes each IP datagram. octet_count must be a value in the range 40 through 18432.

**src { src_host_name | src_host_ip_address }**
Default: originating system’s IP address
Specifies an IP address to use in the packets as the source node.
ping

src_host_name: specifies the source node using the node’s logical host name which must be resolved via DNS lookup.
src_host_ip_address: specifies the source node using the node’s assigned IP address specified using the standard IPv4 dotted decimal notation.

```bash
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in *Command Line Interface Reference*.

**Usage**
This command is useful in verifying network routing and if a remote node is able to respond at the IP layer.

**Example**
The following command is the most basic and will report the results of trying to communication with remote node remoteABC.

```bash
ping remoteABC
```

The following will verify communication with the remote node 1.2.3.4 using 1000 packets.

```bash
ping 1.2.3.4 count 1000
```

The following verifies communication with remote node remoteABC while making it appears as though the source is remote node with IP address 1.2.3.4.

```bash
ping remoteABC src 1.2.3.4
```

**Important**: It is important to note that the responses from the remote host to the ping packets will be rerouted to the host specified as the source.
ping6

Ping options for IPv6 addresses

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
ping6 { hostname | ipv6 address } [ count num ] [ flood ] [ pattern val ] [ size val ] [ src val ] [ interface string ]
```

**hostname**
Name of the host to be pinged.

**ipv6 address**
IPv6 address of host to be pinged.

**count num**
Sets the number of ping packets to be sent. num must be an integer between 1 - 10,000.

**flood**
Configures ping6 to send packets as quickly as possible, or 100 per second, whichever is faster.

**pattern val**
Specifies hex pattern to fill ICMP packets. val is in the range 0x0 - 0xffff

**size val**
Size of ICMP datagram in bytes. val is an integer from 40 - 18432. Default is 56.

**src val**
Specifies the source IP address.

**interface string**
Specifies the originating source interface name.

Usage

Ping command for IPv6. Note that the command is just “ping6, and not “pingv6.”

Example
Use this command to ping the IPv6 address
2001:0db8:85a3:0000:0000:8a2e:0370:7334 ping6
2001:0db8:85a3:0000:0000:8a2e:0370:7334
port

Performs a manual switchover to an available redundant/standby line card or SPIO port.
Default: none.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
port switch to slot#/port#
```

<table>
<thead>
<tr>
<th>slot#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the physical chassis slot where the line card or SPIO card is installed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>port#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the physical port on the line card or SPIO to automatically switch to.</td>
</tr>
</tbody>
</table>

Usage
This command is used to specify the redundant port on a Line Card (LC). When port redundancy is enabled, if an external network device or cable failure occurs that causes a link down failure on the port, then the redundant port is used.

Important: This command is not supported on all platforms.

Example
```
port switch to 17/1
```
ppp echo-test

Verifies the point-to-point link by sending link control protocol packets to the targeted users. This command will not

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator, Operator

Syntax

```
ppp echo-test { callid call_id | imsi imsi_id | ipaddr ip_address | msid ms_id | username user_name } [ num_packets ] [ | ( grep grep_options | more ) ]
```

callid call_id
Specifies the exact call instance ID which is to have its PPP link verified. call_id is specified as a 4-byte hexadecimal number.

imsi imsi_id
Specifies the International Mobile Subscriber Identifier (IMSI) which is to have its PPP link verified.

ipaddr ip_address
Specifies the IP address which is to have its PPP link verified. ip_address must be specified using the standard IPv4 dotted decimal notation.

msid ms_id
Specifies the mobile subscriber ID which is to have its PPP link verified. ms_id must be from 7 to 16 digits specified as an MIN, or RMI.

username user_name
Specifies a user which is to have its PPP link verified. user_name must refer to a previously configured user.

num_packets
Default 1
Specifies the number of test packets to generate. num_packets must be a value in the range from 1 through 1000000.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in Command Line Interface Reference.

Usage
Use the echo test to verify the point-to-point protocol communications.

⚠️ **Caution:** Issuing this command could negatively impact system performance depending on the number of subscribers using the same name and/or if the number of packets used in the test is large.

---

**Example**

The following command tests the PPP link to user `user1`.

```
ppp echo-test username user1
```

The following command tests the PPP link to the user assigned IP address `1.2.3.4`.

```
ppp echo-test ipaddr 1.2.3.4
```

The following tests the PPP link associated with call ID `FE80AA12`.

```
ppp echo-test callid fe80aa12
```
radius interim

Check points current RADIUS accounting messages immediately

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator

Syntax
radius interim accounting now

Usage
The interim command may be part of a regiment of periodic activities to maintain the chassis. This command may also be useful in preparation for system monitoring or troubleshooting to set the list of messages to be displayed at a well known time.
radius test

Verifies the RADIUS servers functions for accounting and authentication.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator

Syntax

```
radius test { accounting | authentication |
probeauthenticationserverip_addriport_no [ username username | password ]
} { all | [ on ] | off } | radius group group_name user_name |
server server_name port server_port } user_name password
```

`accounting`
Test accounting server functionality.

`authentication`
Test authentication server functionality.

`all | radius group group_name user_name | server server_name port server_port`

`all`: indicates all configured servers are to be tested.

`server server_name port server_port`: indicates only the server specified as `server_name` and `server_port` is to be tested. The server must have been previously configured.

`radius group group_name user_name`: tests all configured authentication servers in a specific RADIUS group for specific user. Must be followed by the RADIUS group name and user name.

`group_name` will be a string of size 1 to 63 character and specifies the name of server group configured in specific context for authentication/accounting.

`on/off`
Allows the user to turn radius test accounting on or off.

`user_name`
Specifies the RADIUS user who is to be verified. The user must have been previously configured.

`password`
Specifies the RADIUS user who is to have authentication verified. `password` is only applicable when the `authentication` keyword is specified.

Usage
Test the RADIUS accounting for troubleshooting the system for specific users or to verify all the system RADIUS accounting functions.
Example
The following verifies all RADIUS servers.

```
radius test accounting all
radius test authentication all
```

The following verifies the RADIUS accounting and authentication for user `user1` for the `sampleServer`.

```
radius test accounting server sampleServer port 5000 user1
radius test authentication server sampleServer port 5000 user1 dummyPwd
```

The following commands will verify the RADIUS accounting and authentication for RADIUS server group `star1` for the current context:

```
radius test accounting server sampleServer port 5000 user1
radius test authentication server sampleServer port 5000 user1 dummyPwd
radius test authentication all
```

The following verifies the RADIUS authentication server group `star1` for user `user1`.

```
radius test authentication radius group star1 user1
```

The following displays a sample of the output:

```
Authentication from authentication server 192.168.65.1, port 1812
Authentication Success: Access-Accept received
Round-trip time for response was 29.8 ms
```

The following activates radius test authentication:

```
radius test accounting on group abc server 134.141.12.1 port 1111.
```
reload

Invokes a full system reboot.

Product
All

Privilege
Security Administrator, Administrator

Syntax

reload [ -noconfirm ]

-noconfirm
Execute the command without any additional prompts or confirmation from the user.

Usage
The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the boot system priority command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

Important: To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the reload command. This sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the newcall command in the Exec Mode for additional information.

Caution: Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

Example
The following command performs a hardware reset on the system:

   reload
rename

Changes the name of an existing local file.

Product
All

Privilege
Security Administrator, Administrator

Syntax

rename from_filepath to_filepath [ -noconfirm ]

- from_filepath
  Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:
  - Specifies the source of the copy. url may refer to a local or a remote file. url must be entered using one of the following formats:
    - ASR 5000:
      - [file:][/flash|/pcmcia|/hd][/directory]/file_name

- Important: Use of the SMC hard drive is not supported in this release.

  directory is the directory name
  filename is the actual file of interest

- to_filepath
  Specifies the new name of file/directory. The path must be formatted according to the following formats:
  - Specifies the source of the copy. url may refer to a local or a remote file. url must be entered using one of the following formats:
    - ASR 5000:
      - [file:][/flash|/pcmcia|/hd][/directory]/file_name

- Important: Use of the SMC hard drive is not supported in this release.

  directory is the directory name
  filename is the actual file of interest

- -noconfirm
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

- Important: Extreme caution should be taken when using the -noconfirm option. The paths to the source and the destination should be verified prior to performing the command.
Usage
Rename files as part of regular system maintenance in conjunction with the delete command.

Example
The following renames the directory /pub in the local PCMCIA1 device.

    rename /pcmcia1/pub /pcmcia1/pub_old
reveal disabled commands

Enables the input of commands for features that do not have license keys installed. The output of the command `show cli` indicates when this is enabled. This command affects the current CLI session only. This is disabled by default.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
reveal disabled commands

no reveal disabled commands
```

**Usage**

When this is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command. When this is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

**Example**

Set the CLI to accept disabled commands and display the required feature for the current CLI session with the following command:

```
reveal disabled commands
```

Set the CLI to reject disabled commands and return an error message for the current CLI session:

```
no reveal disabled commands
```
rlogin

Attempts to connect to a remote host.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax
```
rlogin { host_name | host_ip_address } [ user user_name ]
```

- `host_name | host_ip_address`
  Identifies the remote node to attempt to connect to.
  - `host_name`: specifies the remote node using the node’s logical host name which must be resolved via DNS lookup.
  - `host_ip_address`: specifies the remote node using the node’s assigned IP address specified using the standard IPv4 dotted decimal notation.

- `user user_name`
  Specifies a user name to attempt to connect as. `user_name` must be from to 1023 alpha and/or numeric characters.

Usage
Connect to remote network elements using rlogin.

**Important:** *rlogin* is not a secure method of connecting to a remote host. *ssh* should be used whenever possible for security reasons.

Example
The following connects to remote host `remoteABC` as user `user1`.

```
rlogin remoteABC user user1
```

The following connects to remote host `1.2.3.4` without any default user.

```
rlogin 1.2.3.4
```
rmdir

Removes (deletes) a local directory.

Product
All

Privilege
Security Administrator, Administrator

Syntax

rmdir path [ force ]

path
Specifies the directory path to remove. The must be formatted according to the following formats:
Specifies the source of the copy. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats:
directory is the directory name
directory is the actual file of interest

force
Over-rides any warnings to force deletion of the directory and any files contained therein.

Important: Use of the *force* keyword should be done with care to ensure the directory is specified accurately as there is no method to recover a directory which has been removed.

Usage
Remove old directories as part of regular maintenance.

Example
The following removes the local directory `/pcmcia1/pub`

    rmdir /pcmcia1/pub
rotate-hd-file

This command rotates the current temp file manually.

Product
SGW, PGW, HSGW

Privilege
Security Administrator, Administrator

Syntax

```
rotate-hd-file [ name policy_name ]

[ name policy_name ]

Specifies the hd-storage policy name. policy_name must be an existing HD Storage Policy name and must be an alpha and/or numeric string of 0 through 63 characters in length.
```

Usage
Use this command to manually rotate the Diameter HD stored files.

Example
The following command rotates Diameter files in the HD storage drive for files stored using the HD storage policy named CDR1:

```
rotate-hd-file diameter name CDR1
```
save configuration

Saves the current contexts configuration to a local or remote location.

Product
All

Privilege
Security Administrator, Administrator

Syntax

save configuration url [ -redundant ] [ -noconfirm ] [ showsecrets ] [ verbose ]

url
Default: saves to the location of the active configuration currently loaded.
Specifies the location to store the configuration file(s). url may refer to a local or a remote file. url must be entered using one of the following formats:
Specifies the source of the copy. url may refer to a local or a remote file. url must be entered using one of the following formats:

- \[file:\] [/flash|/pcmcia1|/hd] [/directory] /file_name
- [ ftp: | sftp: ] // [username[ :password@] ] [host] [ :port# ] [ /directory] /file_name

directory is the directory name.
filename is the actual file of interest.

**Important:** Configuration files should be named with a .cfg extension.

username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.

**Important:** hostname can only be used if the networkconfig parameter is configured for DHCP and the DHCP server returns a valid nameserver.

port# is the logical port number that the communication protocol is to use.

**-redundant**
This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the standby processing card, if available.

**Important:** This keyword will only work for local devices that are located on both the active and standby processing cards. For example, if you save the file to the /pcmcia1 device on the active processing card, that same type
of device (card in Slot 1 of the standby processing card) must be available. Otherwise, a failure message is displayed. If saving the file to an external network (non-local) device, the system disregards this keyword.

**Important:** This keyword does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active processing card, then you must synchronize the local file system on both SMC cards.

- **noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Important:** Caution should be exercised when using the **noconfirm** option as this may cause the accidental over-write of data if the URL refers to an existing file.

- **showsecrets**
  This keyword causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.

- **verbose**
  Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**Usage**
Backup the current configuration as part of periodic maintenance activities in case of emergencies.

**Important:** The saving of a configuration does not save the boot options as configured via the global configuration mode **boot** commands.

**Example**
The following saves the configuration data to the local file `/flash/pub/juneconfig.cfg` with no confirmation from the user:

```
save configuration /flash/pub/juneconfig.cfg -noconfirm
```

The following saves the configuration data to remote hoist `remoteABCas /pub/juneconfig.cfg`:

```
save configuration tftp://remoteABC/pub/juneconfig.cfg
```
save logs

Saves the current log file to a local or remote location.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
save logs { url } [ active ] [ inactive ] [ callid call_id ] [ event-verbosity evt_verboseness ] [ facility facility ] [ level severity_level ] [ pdu-data pdu_format ] [ pdu-verbosity pdu_verboseness ] [ since from_date_time [ until to_date_time ] ] [ | { grep grep_options | more } ]
```

- **url**
  Specifies the location to store the log file(s). `url` may refer to a local or a remote file. `url` must be entered using one of the following formats:
  - Specifies the source of the copy. `url` may refer to a local or a remote file. `url` must be entered using one of the following formats:

```
directory
filename
username
password
host
```

- **Important:** Use of the SMC hard drive is not supported in this release.

```
directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
```

```
Important: hostname can only be used if the networkconfig parameter is configured for DHCP and the DHCP server returns a valid nameserver.
```

- **port#** is the logical port number that the communication protocol is to use.

- **active**
  Indicates output is to display data from active logs.

- **inactive**
  Indicates output is to display data from inactive logs.

- **callid call_id**
  Specifies a call ID for which log information is to be displayed. `call_id` must be specified as a 4-byte hexadecimal number.
**event-verbosity evt_verbosity**

Specifies the level of verboseness to use in displaying of event data as one of:

- `min` - displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- `concise` - displays detailed information about the event, but does not provide the event source within the system.
- `full` - displays detailed information about event, including source information, identifying where within the system the event was generated.

**facility facility**

Specifies the facility to modify the filtering of logged information for as one of:

- `a10`: A10 interface facility
- `a11`: A11 interface facility
- `a11mgr`: A11 Manager facility
- `aaa-client`: AAA client facility
- `aaamgr`: AAA manager logging facility
- `aaaproxy`: AAA Proxy facility
- `acl-log`: Access Control List logging facility
- `acsctrl`: Active Charging Service (ACS) Controller facility
- `acsmgr`: Active Charging Service (ACS) Manager facility
- `alarmctrl`: Alarm Controller facility
- `all`: All facilities
- `asf`: Voice Application Server Framework logging facility
- `asfprt`: ASF Protocol Task (SIP) logging facility
- `asngwmgr`: ASN Gateway Manager facility
- `asnpemgr`: ASN Paging/Location-Registry Manager facility
- `bgp`: Border Gateway Protocol (BGP) facility
- `cli`: CLI logging facility
- `cscf`: IMS/MMD CSCF
- `cscfmg`: SIP CSCF Manager facility
- `csp`: Card Slot Port controller facility
- `css`: Content Service Selection (CSS) facility
- `css-sig`: Content Service Selection (CSS) RADIUS Signaling facility
- `dcardctrl`: IPSEC Daughtercard Controller logging facility (not used at this time)
- `dcardmgr`: IPSEC Daughtercard Manager logging facility (Not used at this time)
- `dhcp`: DHCP facility (GGSN product only)
- `dhost`: Distributed Host logging facility
- `diameter`: Diameter endpoint logging facility
- `diameter-acct`: Diameter Accounting
• **diameter-auth**: Diameter Authentication
• **diameter-ecs**: ECS Diameter signaling facility
• **diameter-svc**: Diameter Service
• **diamproxy**: DiamProxy logging facility
• **dpath**: IPSEC Data Path facility
• **drvctrl**: Driver Controller facility
• **evlog**: Event log facility
• **famgr**: Foreign Agent manager logging facility
• **firewall**: Firewall logging facility
• **gss-gcdr**: GTPP Storage Server GCDR facility
• **gtpc**: GTP-C protocol logging facility (GGSN product only)
• **gtpcmgr**: GTP-C protocol Manager logging facility (GGSN product only)
• **gtpp**: GTP-PRIME protocol logging facility (GGSN product only)
• **gtpu**: GTP-U protocol logging facility (GGSN product only)
• **h248p**: H.248 Protocol logging facility
• **hamgr**: Home Agent manager logging facility
• **hat**: High Availability Task (HAT) process facility
• **ims-authorizatn**: IMS Authorization Service facility
• **ip-arp**: IP Address Resolution Protocol facility
• **ip-interface**: IP interface facility
• **ip-route**: IP route facility
• **ipsec**: IP Security logging facility
• **ipsgmgr**: IP Services Gateway facility
• **ipsp**: IP Pool Sharing Protocol logging facility
• **l2tp-control**: L2TP control logging facility
• **l2tp-data**: L2TP data logging facility
• **l2tpdemux**: L2TP Demux Manager logging facility
• **l2tpmgr**: L2TP Manager logging facility
• **li**: Lawful intercept facility (Logs are visible only to system accounts with li-administrator privileges.)
• **mme-app**: MME application facility
• **mme-hss**: MME HSS Service facility
• **mme-misc**: MME miscellaneous logging facility
• **mmedemux**: MME Demux Manager logging facility
• **mmemgr**: MME Manager logging facility
• **mmgr**: SGSN/SS7 Master Manager logging facility
• **mobile-ip**: Mobile IP processes
• **mobile-ip-data**: Mobile IP data facility
- **multicast-proxy**: Multicast Proxy logging facility
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npumgr**: Network Processor Unit Manager facility
- **nsctrl**: Charging Service Controller facility (supported in conjunction with ECSv1)
- **nsmgr**: Charging Service Manager facility
- **nsproc**: Charging Service process facility
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF logging facility
- **ppp**: PPP link and packet facilities
- **radius acct**: RADIUS accounting logging facility
- **radius auth**: RADIUS authentication logging facility
- **radius coa**: RADIUS change of authorization and radius disconnect
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rip**: RIP logging facility (RIP is not supported at this time.)
- **rohc**: RObust Header Compression facility
- **rsvp**: Reservation Protocol logging facility
- **sct**: Shared Configuration Task logging facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sft**: Switch Fabric Task logging facility
- **sipcdprt**: Sip Call Distributor facility
- **sitmain**: System Initialization Task main logging facility
- **snmp**: SNMP logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **ssh ipsec**: SSH IP Security logging facility
- **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **threshold**: threshold logging facility
- **udr**: User detail record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **vpn**: Virtual Private Network logging facility
- `wimax-data`: WiMAX DATA
- `wimax-r6`: WiMAX R6

### level severity_level
Specifies the level of information to be logged, severity_level, from the following list which is ordered from highest to lowest:
- `critical`: display critical events
- `error`: display error events and all events with a higher severity level
- `warning`: display warning events and all events with a higher severity level
- `unusual`: display unusual events and all events with a higher severity level
- `info`: display info events and all events with a higher severity level
- `trace`: display trace events and all events with a higher severity level
- `debug`: display all events

### pdu-data pdu_format
Specifies output format for the display of packet data units as one of:
- `none`: output is in raw format (unformatted).
- `hex`: output being displayed in hexadecimal format.
- `hex-ascii`: output being displayed in hexadecimal and ASCII similar to a main-frame dump.

### pdu-verbosity pdu_verboseness
Specifies the level of verboseness to use in displaying of packet data units as a value from 1 to 5 where 5 is the most detailed.

### since from_date_time [ until to_date_time ]
Default: no limit.
since from_date_time: indicates only the log information which has been collected more recently than from_date_time is to be displayed.
until to_date_time: indicates no log information more recent than to_date_time is to be displayed. until defaults to current time when omitted.
from_date_time and to_date_time must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where YYYY is a 4-digit year, MM is a 2-digit month in the range 01 through 12, DD is a 2-digit day in the range 01 through 31, HH is a 2-digit hour in the range 00 through 23, mm is a 2-digit minute in the range 00 through 59, and ss is a 2 digit second in the range 00 through 59.
to_date_time must be a time which is more recent than from_date_time.
The use of the until keyword allows for a time range of log information while only using the since keyword will display all information up to the current time.

### grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in Command Line Interface Reference.
Usage
Backup the current log file as part of periodic maintenance activities.

Example
The following saves the log to the local file /flash/pub/junelogs.logs with no confirmation from the user:

```bash
save logs /flash/pub/junelogs.logs -noconfirm
```

The following saves the configuration data to remote host remoteABC as /pub/junelogs.logs:

```bash
save logs tftp://remoteABC/pub/junelogs.logs
```
session trace subscriber

This command enable disables the subscriber session trace functionality based on a specified subscriber device or ID on one or all instance of session on a specified EPS network elements.

**Product**
MME, P-GW, S-GW

**Privilege**
Operator

**Syntax**

```
session trace subscriber network-element {mme | pgw | sgw} {imei id} {imsi id} {interface {all | interface}} trace-ref id collection-entity ip_address
```

```
no session trace subscriber [network-element {mme | pgw | sgw}] [trace-ref id]
```

**no**
Disables the entire session trace or for a specific network element and/or trace reference.

**network-element { mme | pgw | sgw }**

Identifies the network element that, in turn, identifies the interfaces where the session trace is to occur. Specific interfaces can be specified using the interface keyword described below.

- **mme**: Specifies that the session trace is to occur on one or all interfaces on the MME.
- **pgw**: Specifies that the session trace is to occur on one or all interfaces on the P-GW.
- **sgw**: Specifies that the session trace is to occur on one or all interfaces on the S-GW.

**imei id**

Specifies the International Mobile Equipment Identification number of the subscribers UE. *id* must be the 8 digit TAC (Type Allocation Code) and 6 digit serial number. Only the first 14 digits of the IMEI/IMEISV are used to find the equipment ID.

**imsi id**

Specifies the International Mobile Subscriber Identification (IMSI). *id* must be the 3 digit MCC (Mobile Country Code), 2 or 3 digit MNC (Mobile Network Code), and the MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits.

**interface { all | interface }**

Specifies the interfaces where the session trace application will collect data.

- **all**: Specifies that all interfaces associated with the selected network element
- **interface**: Specifies the interface type where the session trace application will collect trace data. The following interfaces are applicable for the network element type:
  - **MME**:
    - **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
    - **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
• **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.

• **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.

• **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.

• **P-GW:**

  • **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.

  • **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.

  • **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.

  • **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.

  • **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.

  • **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.

  • **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.

  • **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

• **S-GW:**

  • **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.

  • **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.

  • **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.

  • **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.

  • **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

---

**trace-ref** *id*

Specifies the trace reference for the trace being initiated. *id* must be the MCC (3 digits), followed by the MNC (3 digits), then the trace ID number (3 byte octet string).

**collection-entity** *ip_address*

Specifies the IP address of the collection entity where session trace data is pushed. *ip_address* must be a valid IPv4 address and is specified in dotted decimal notation.
Usage

Use this command to initiate a session trace for a specified subscriber device or ID on one or all interfaces on a specified network element.

Important: Session trace configuration is performed in the Global Configuration Mode using the `session trace` command. Refer to the Global Configuration Mode Commands chapter in this reference for more information.

Example

The following command initiates a session trace on a P-GW S5 interface for a subscriber with an IMSI of 322233123456789 and sets the trace reference as 322233987654 and the collection entity IP address as 1.2.3.4:

```
session trace subscriber network-element pgw imsi 322233123456789
interface s5 trace-ref 322233987654 collection-entity 1.2.3.4
```

The following command initiates a session trace on an MME S6a interface for a subscriber with an IMSI of 322233123456789 and sets the trace reference as 322233987654 and the collection entity IP address as 1.2.3.4:

```
session trace subscriber network-element mme imsi 322233123456789
interface s6a trace-ref 322233987654 collection-entity 1.2.3.4
```
setup

Enters the system setup wizard which guides the user through a series of questions regarding the system basic configuration options such as initial context-level administrative users, host name, etc.

Product
All

Privilege
Security Administrator, Administrator

Syntax

setup

Usage
The setup wizard provides a user friendly interface for initial system configuration.

⚠️ Important: If the configuration script generated by the setup wizard is applied when an existing configuration is in use the options which are common to both are updated and all remaining options are left unchanged.

Example

setup
sgsn imsigr

Enters commands to manage the SGSN IMSIMgr audits.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sgsn imsigr { add-record imsi sessmgr instance sessmgr# | audit-with sessmgr { all | instance sessmgr# } | remove-record imsi }
```

**add-record imsi**

Adds a record for an IMSI to the IMSI manager’s audit table and associates a specific Session Manager (SessMgr) with the IMSIMgr for the IMSI audit.

- **imsi** - enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

**sessmgr instance sessmgr#**

Identifies a specific Session Manager (SessMgr) to associate with the IMSIMgr for the IMSI audit.

- **sessmgr#** - enter up to 4 digits, 0 to 4095.

**audit-with sessmgr { all | instance sessmgr# }**

Initiate an IMSI audit with a specific Session Manager (SessMgr) or with all SessMgs.

- **sessmgr#** - enter up to 4 digits, 0 to 4095.

**remove-record**

Delete a specific IMSI from the IMSI audit table.

- **imsi** - enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

**Usage**

Use this command to manage the IMSIMgr’s audit functions. Associate one or multiple SessMgs with the IMSIMgr for the audits.

**Example**

```
sgsn imsigr audit-with sessmgr instance 245
```
sgsn offload

This command configures the offloading procedure and actually starts and stops the offloading of subscribers which is part of the SGSN’s Gb flex load redistribution functionality.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sgsn offload gprs-service srcv_name { activating | connecting } [ nri-value | stop | t3312-timeout seconds]
```

**srcv_name**
A unique string of 1 to 63 alphanumeric characters that identifies a specific GPRS service.

**activating**
Instructs the SGSN to offload any subscribers sending an ‘activate request’ message.

**connecting**
Instructs the SGSN to offload any subscribers sending either an ‘attach request’ or a ‘RAU request’ message.

**nri-value**
Instructs the SGSN to check the P-TMSI and use the SGSN matching the configured NRI value to offload subscribers

**stop**
Instructs the SGSN to stop offloading subscribers from the pool area.

**t3312-timeout**
Configures the timer for sending period RAUs to the MS. Default is 4 seconds.

*seconds*: Must be an integer from 2 to 60.

Usage
Use this command to configured the offloading of subscribers which is a part of the SGSN’s load redistribution operation. This command can be used anytime an SGSN is to be taken out of service.

Example
The following command instructs the SGSN to notify all MS to detach and reattach.

```
sgsn offload gprs-service srcv_name activating nri-value nri_value
```
shutdown

Terminates all processes within the chassis.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
shutdown [ -noconfirm ]
```

- **-noconfirm**
  Execute the command without any additional prompts or confirmation from the user.

Usage

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the `boot system priority` command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

**Important:** To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the `shutdown` command. This sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the `newcall` command in the Exec Mode for additional information.

**Caution:** Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

Example

The following command performs a hardware reset on the system:

```
shutdown
```
sleep

Pauses the CLI interface.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
sleep seconds
```

`seconds`

Specifies the number of seconds to pause. The number of seconds must be a value in the range from 1 through 3600.

Usage
Sleep is a command delay which is only useful when creating command line interface scripts such as predefined configuration files/scripts.

Example
The following will cause the CLI to pause for 30 seconds.

```
sleep 30
```
**srp initiate-switchover**

This command changes the device status on the primary and backup HA or GGSN systems configured for Interchassis Session Recovery support.

**Product**
HA, GGSN PDIF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
srp initiate-switchover [ post-processing-timeout | reset-route-modifier | timeout seconds ] [ -noconfirm ]
```

- **post-processing-timeout**
  Specifies the timeout value in seconds to initiate the post-switchover process. The value must be an integer from 0 through 3600.

- **reset-route-modifier**
  During a switchover, reset the route-modifier to the initial value.

- **timeout seconds**
  Default: 300
  Specifies the number of seconds before a forced switchover occurs. seconds must be a value in the range from 0 through 65535.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

This command executes a forced switchover from active to inactive. The command must be executed on the active system and switches the active system to the inactive state and the inactive system to an active state.

**Example**

The following initiates a switchover in 30 seconds.

```
srp initiate-switchover timeout 30
```
srp reset-auth-probe-fail

This command resets the auth probe monitor failure information.

**Product**
HA, GGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**
```
srp reset-auth-probe-fail
```

**Usage**
This command resets the auth probe monitor failure information to 0.
srp terminate-post-process

This command forcibly terminates the post-switchover of primary and backup HA or GGSN systems configured for Interchassis Session Recovery (ICSR) support.

Product
HA, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
srp terminate-post-process [ -noconfirm ]

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Use this command to force the termination of post-switchover process.

Example
srp terminate-post-process
srp validate-configuration

Initiates a configuration validation check from the ACTIVE chassis.

**Product**
- HA, GGSN PDIF

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
srp validate-configuration
```

**Usage**

Validates the configuration for an active chassis.
**ssh**

Connects to a remote host using a secure interface.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```plaintext
ssh { host_name | host_ip_address } [ port port_num ] [ user user_name ]
```

- **host_name / host_ip_address**
  Identifies the remote node to attempt to connect to.
  *host_name*: specifies the remote node using the node’s logical host name which must be resolved via DNS lookup.
  *host_ip_address*: specifies the remote node using the node’s assigned IP address specified using the standard IPv4 dotted decimal notation.

- **port port_num**
  Specifies a specific port to connect to where *port_num* must be a value in the range 1025 through 10000.

- **user user_name**
  Specifies a user name to attempt to connect as.

**Usage**

SSH connects to a remote network element using a secure interface.

**Example**

The following connects to remote host `remoteABC` as user `user1`.

```plaintext
ssh remoteABC user user1
```

The following connects to remote host `1.2.3.4` without any default user.

```plaintext
ssh 1.2.3.4
```

The following connects to remote host `1.2.3.4` via port `2047` without any default user.

```plaintext
ssh 1.2.3.4 port 2047
```
start crypto security-association

Initiates IKE negotiations.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
start crypto security-association cryptomap
```

`cryptomap`

This is the name of the crypto map policy to use when starting the IKE negotiations. `cryptomap` must be the name of an existing crypto map entered as an alpha and/or numeric string of from 1 to 127 characters.

**Usage**

Use this command to start IKE negotiations for IPSEC.

**Example**

The following command starts the IKE negotiations using the parameters set in the crypto map named `cryptomap1`:

```
start crypto security-association cryptomap1
```
Chapter 91
Exec Mode (T-Z)

This section includes the commands `telnet` through `upgrade url-blacklisting database`. 
**telnet**

Connects to a remote host using the terminal-remote host protocol.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
telnet { host_name | host_ip_address } [ port port_num ]
```

- `host_name | host_ip_address`
  
  Identifies the remote node to attempt to connect to.
  
  - `host_name`: specifies the remote node using the node’s logical host name which must be resolved via DNS lookup.
  
  - `host_ip_address`: specifies the remote node using the node’s assigned IP address specified using the standard IPv4 dotted decimal notation.

- `port port_num`
  
  Specifies a specific port to connect to where `port_num` must be a value in the range 1025 through 10000.

**Usage**

Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.

**Important**: `telnet` is not a secure method of connecting between two hosts. `ssh` should be used whenever possible for security reasons.

**Example**

The following connects to remote host `remoteABC`.

```
telnet remoteABC
```

The following connects to remote host `1.2.3.4` port `2047`.

```
telnet 1.2.3.4 port 2047
```
terminal

Sets the number of rows or columns for output.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
terminal { length lines | width characters }
```

- `length lines`: sets the terminal length in number of `lines` (rows) of text from 5 to 4294967295 lines or the special value of 0 (zero). The value 0 sets the terminal length to infinity.
- `width characters`: sets the terminal width in number of `characters` from 5 to 512 characters.

Usage

Set the length to 0 (infinite) when collecting the output of a command line interface session which is part of a scripted interface.

Example

The following sets the length then width in two commands.

```
terminal length 66
terminal width 160
```

The following command sets the number of rows of the terminal to infinity.

```
terminal length 0
```
test alarm

Tests the alarm capabilities of the chassis.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
test alarm { audible | central-office { critical | major | minor } }
```

- **audible | central-office { critical | major | minor }**
  - **audible**: indicates that the internal alarm on the system management card is to be tested for 10 seconds. The alarm status is returned to its prior state, i.e., if the audible alarm was enabled prior to the test, the alarm will again be enabled following the test.
  - **central-office { critical | major | minor }**: indicates the central office alarms are to be tested for the specified CO alarm.

Usage

Test the alarm capabilities of the chassis as periodic maintenance to verify the hardware for generation of the internal audible alarms is functional.

Example

```
test alarm audible
test alarm central-office critical
test alarm central-office major
test alarm central-office minor
```
timestamps

Enables/disables the generation of a timestamp in response to each command entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects the current CLI session only. Use the `timestamps` command in the Global Configuration Mode to change the behavior for all future CLI sessions.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
timestamps

no timestamps
```

```
no

Disables generation of timestamp output for each command entered. When omitted, the output of a timestamp for each entered command is enabled.
```

Usage
Enable timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.
traceroute

Collects information on the route data will take to a specified host.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Important: Inspector privileges are granted for all variables except count and port. To initiate a traceroute count or to target a specific port for a traceroute, you must have a minimum privilege level of Operator.

Syntax

```
traceroute { host_name | host_ip_address } [ count packets ] [ df ] [ maxttl max_ttl ] [ minttl min_ttl ] [ portport_num ] [ sizersoctet_count ] [ src { src_host_name | src_host_ip_address } ] [ timeoutseconds ] [ | { grep grep_options | more } ]
```

**host_name | host_ip_address**
Identifies the remote node to trace the route to.
*host_name*: specifies the remote node using the node’s logical host name which must be resolved via DNS lookup.
*host_ip_address*: specifies the remote node using the node’s assigned IP address specified using the standard IPv4 dotted decimal notation.

**count packets**
Default: 3
Specifies the number of UDP probe packets to send.

**df**
Indicates the packets for the tracing of the route should not be fragmented. If a packet would require fragmenting then it is dropped and the result is the ICMP response “Unreachable, Needs Fragmentation” is received.

**maxttl max_ttl**
Default: 30
Specifies the maximum time to live, in seconds, for the route tracing packets. *max_ttl* must be specified as a value in the range of 1 through 255. It is an error if *max_ttl* is less than *min_ttl* whether *min_ttl* is specified or defaulted.
The time to live (TTL) is the number of hops through the network, i.e., it is not a measure of time.

**minttl min_ttl**
Default: 1
Specifies the minimum time to live, in seconds, for the route tracing packets. \texttt{min\_ttl} must be specified as a value in the range of 1 through 255. It is an error if \texttt{min\_ttl} is greater than \texttt{max\_ttl} whether \texttt{max\_ttl} is specified or defaulted. The time to live (TTL) is the number of hops through the network, i.e., it is not a measure of time.

\begin{verbatim}
port port_num
\end{verbatim}

Default: 33434
Specifies a specific port to connect to where \texttt{port\_num} must be a value in the range 1 through 65535.

\begin{verbatim}
size octet_count
\end{verbatim}

Default: 40
Specifies the number of bytes each packet. \texttt{octet\_count} must be a value in the range 40 through 32768.

\begin{verbatim}
src \{ src\_host\_name | src\_host\_ip\_address \}
\end{verbatim}

Default: originating system’s IP address
Specifies an IP address to use in the packets as the source node.
\texttt{src\_host\_name}: specifies the remote node using the node’s logical host name which must be resolved via DNS lookup.
\texttt{src\_host\_ip\_address}: specifies the remote node using the node’s assigned IP address specified using the standard IPv4 dotted decimal notation.

\begin{verbatim}
timeout seconds
\end{verbatim}

Default: 5
Specifies the maximum time to wait for a response from each route tracing packet. \texttt{seconds} must be a value in the range 2 through 100.

\begin{verbatim}
grep grep\_options | more
\end{verbatim}

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of \texttt{grep} and \texttt{more}, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series-series Command Line Interface Reference.

### Usage

Trace an IP route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

### Example

The following traces the route to remote host \texttt{remoteABC} and sends the output to the more command.

\begin{verbatim}
traceroute remoteABC | more
\end{verbatim}

The following command traces the route to remote host 1.2.3.4’s port 2047 waiting a maximum of 2 seconds for responses.

\begin{verbatim}
traceroute 1.2.3.4 port 2047 timeout 2
\end{verbatim}
traceroute
**update active-charging**

This command updates specified active charging option(s) for the matching sessions.

**Product**
ACS, FW, NAT

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
update active-charging { switch-to-fw-and-nat-policy fw_nat_policy | switch-to-rulebase rulebase } { all | callid call_id | fw-and-nat-policy fw_nat_policy | imsi imsi | ip-address ipv4_address | msid msid | rulebase rulebase | username user_name } [ -noconfirm ] [ | { grep grep_options | more } ]
```

---

**switch-to-fw-and-nat-policy**
Switch to the specified Firewall-and-NAT policy.
`fw_nat_policy` must be a string of 1 through 63 characters in length.

---

**switch-to-rulebase**
Switch to the specified rulebase.
`rulebase` must be a string from 1 through 63 characters in length.

---

**all**
Updates rulebase for all subscribers.

---

**callid call_id**
Specific Call identification number.
`call_id` must be an eight-digit HEX number.

---

**fw-and-nat-policy fw_nat_policy**
Specific Firewall-and-NAT policy.
`fw_nat_policy` must be a string from 1 through 63 characters in length.

---

**imsi imsi**
Specific International Mobile Subscriber Identification (IMSI).
`imsi` must be 3 digits of MCC (Mobile Country Code), 2 or 3 digits of MNC (Mobile Network Code), and the rest with MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits. For example, 123-45-678910234 can be entered as 12345678910234.

---

**ip-address ipv4_address**
Specific IPv4 IP address.
`ipv4_address` must be IPv4 address in dotted decimal notation.
**update active-charging**

**msid msid**
Updates rulebase for a specific MSID.  
*msid* must be a string of 1 through 24 characters in length.

**rulebase rulebase**
Updates rulebase for sessions matching the specified rulebase.  
*rulebase* must be a string from 1 through 63 characters in length.

**username user_name**
Updates rulebase for a specific user.  
*user_name* must be a sequence of characters and/or wildcard characters ("\$" and "\*") - string of 1 through 127 characters in length.

**-noconfirm**
Specifies that the command is to execute without any additional prompt and confirmation from the user.

```
| \{ grep grep_options | more \}
```
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.  
For details on the usage of *grep* and *more*, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
Use this command to change specified active charging option(s) for the matching sessions.

**Example**
The following command changes the rulebase for sessions using the rulebase named *standard* to use the rulebase named *super*:

```
update active-charging switch-to-rulebase super rulebase standard
```
**update cscf**

This command will cause a NOTIFY to be triggered from S-CSCF with contact event as “shortened” and indicating the expiry timer value for each contact as “reauthentication-time” provided from CLI. The subscriber is supposed to send a fresh REGISTER message within “reauthentication-time”, which will be challenged by S-CSCF in order to accomplish reauthentication. If reauthentication does not occur/fails, the subscriber will be cleared after “reauthentication-time”.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Syntax**

```
update cscf subscriber { all | username user_name } cscf-service service_name
reauthentication-time seconds [ verbose ]
```

- **subscriber { all | username user_name }**
  Updates cscf subscriber data.
  all: Updates data for all subscribers within a specified S-CSCF service.
  username **user_name**: Name of specific user within current context. can be between 1 and 127 alpha and/or numeric characters and is case sensitive.

- **cscf-service service_name**
  Specific configured S-CSCF service. **service_name** can be between 1 and 63 alpha and/or numeric characters and is case sensitive.

- **reauthentication-time seconds**
  Specify the time within which subscriber is expected to reauthenticate. **seconds** must be an integer from 1 to 86400 seconds.

- **verbose**
  Show detailed information.

**Usage**
This command is only applicable for an S-CSCF service.

**Important:** reauthentication-time should be greater than the current expiry time of the contact so that S-CSCF will initiate the NOTIFY message.

**Example**
The following command sets the reauthentication time for all CSCF subscribers in the **scsf1** S-CSCF service to **500** seconds:

```
update cscf subscriber all cscf-service scsf1 reauthentication-time 500
```
update firewall policy

This command is obsolete.
update ip

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

update ip access-list list_name subscribers [ command_keyword ] [ filter_keywords ] [ | { grep grep_options | more } ]

list_name
This is the name of the IP Access list that you want to apply to the subscriber.

[ command_keyword ] [ filter_keywords ]
These are the same command keywords and filter keywords available for the show subscribers command.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to force existing subscriber sessions that are already using a specific IP Access list to have that IP Access list reapplied. This is useful when you edit an IP Access list and want to make sure that even existing subscriber sessions have the new changes applied.

Example
To apply the IP Access list named ACLlist1 to all existing subscribers that are already using that IP Access list, enter the following command:

update ip access-list ACLlist1 subscribers all
update qos policy map

Updates QoS profile information based on specific subscriber policy maps.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
update qos policy-map map_name use-granted-profile-id id1 [ id2 ] [ id3 ]
subscribers [ command_keyword ] [ filter_keywords ] [ -noconfirm ] [ verbose ] [ match-requested-profile-id ] [ | { grep grep_options | more } ]
```

- **map_name**
  Specifies the name of the policy map. `map_name` can be from 1 to 15 alpha and/or numeric characters in length.

- **use-granted-profile-id id1 [ id2 ] [ id3 ]**
  Specifies the profile IDs to update. Up to 3 different profile IDs can be specified. Each profile ID is specified as a hexadecimal value from 0x0 and 0xFFFF.

- **subscribers [ command_keyword ] [ filter_keywords ]**
  These are the same command keywords and filter keywords available for the `show subscribers` command.

- **[ -noconfirm ]**
  Updates matching subscribers without prompting for confirmation.

- **[ verbose ]**
  Displays details for the profile updates.

- **[ match-requested-profile-id ]**
  Causes the system to send session-updates only with profile-ids matching the profile-ids in the requested list.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

**Usage**

Use this command to update subscriber session profile IDs based on the specified criteria.
Example
The following command updates profile IDs 0x3E and 0x4C for all subscriber sessions and sends session-updates with the IDs:

```
update qos policy-map test use-granted-profile-id 0x3E 0x4C subscribers all match-requested-profile-id
```
**update qos tft**

Updates the subscribers TFT associated with the flow ID and direction.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
update qos tft flow-id flow-id flow-dir {forward | reverse} use-granted-profile-id id1[id2] [id3] subscribers [ command_keyword ] [ filter_keywords ][-noconfirm ] [ verbose ] [ match-requested-profile-id ] [ | { grep|grep_options | more }
```

- **flow-id**
  
  When `flow-id` is specified, the session update will be sent only when the flow ID matches the flow-id and flow-direction. The `flow-id` must be specified as a value in the range of 1 through 255.

- **flow-dir {forward | reverse}**
  
  The direction of the tft flow.

- **subscribers [ command_keyword ] [ filter_keywords ]**
  
  These are the same command keywords and filter keywords available for the `show subscribers` command.

**Usage**

Supports QoS updates based on subscriber TFTs.

**Example**

```
update qos tft flow-id 0 flow-dir reverse use-granted-profile-id 0x0 subscribers all -noconfirm
```
**upgrade**

This command installs major software releases to the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
upgrade { online | patch } image_url config_url [ -noconfirm ]
```

<table>
<thead>
<tr>
<th><strong>Keyword</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>online</strong></td>
<td>Perform a software upgrade from one release version to another. The online upgrade is only available for software release 3.5 and higher.</td>
</tr>
<tr>
<td><strong>patch</strong></td>
<td>Install an interim, or patch, software release.</td>
</tr>
</tbody>
</table>

**Important:** Software Patch Upgrades are not supported in this release.

**image_url**

Specifies the location of an image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted according to one of the following formats:

- ASR 5000:
  
  ```
  *[file: ]{/flash|/pcmcia1|/hd}/{directory}\/file_name
  *[ http: | tftp: ]\//{ host[ :port# ]}{ /directory }/file_name
  ```

  - `directory` is the directory name.
  - `filename` is the actual file of interest.
  - `host` is the IP address or host name of the server.
  - `port#` is the logical port number that the communication protocol is to use.

**Important:** A file intended for use on an ASR 5000 uses the convention `xxxxx.ASR5000.bin`, where `xxxxx` is the software build information.

**Important:** When using the TFTP, it is advisable to use a server that supports large blocks, per RFC 2348. This can be implemented by using the “block size option” to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

**config config_path**

Specifies the location of a configuration file to use for system startup. This must be formatted according to the following format:

- ASR 5000:
upgrade

*file: */flash|/pcmcia|/hd|[/path]/filename

Where path is the directory structure to the file of interest, and filename is the name of the configuration file. This file typically has a .cfg extension.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use the upgrade online command to perform a software upgrade when upgrading from one software release version to another, providing that both versions support this feature. For example, you can use this method to upgrade from release version 3.5 (any build number) to version 4.0 (any build number), but you cannot use this method to upgrade from release version 3.0 to version 3.5 since version 3.0 does not support the feature.

**Important:** Software Patch Upgrades are not supported in this release.

**Important:** This command is not supported on all platforms.

**Example**

The following command performs a major software release upgrade from an older version to a newer version. In this example the new software image file is in a subdirectory on a tftp server, and the configuration file is in a subdirectory on the local flash.tftp://host[/path]/filename

    upgrade online tftp://imageserver/images/image.bin config
    /flash/configurations/localconfig.cfg
upgrade content-filtering

This command upgrades the Static Rating Database (SRDB) for Category-based Content Filtering application.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

```
upgrade content-filtering category { database | rater-pkg }
```

- **upgrade content-filtering category database**
  This command triggers upgrade of the Category-based Content Filtering Static Rating Database (SRDB).

- **upgrade content-filtering category rater-pkg**
  This command triggers manual upgrade of the Dynamic Content-Filtering Rater Package (rater.pkg file). The rater.pkg file contains the models and feature counters that are used to return the dynamic content rating. The upgrade will trigger distribution of the rater.pkg to all the SRDBs.

Usage

Use this command to load the Static Rating Database (SRDB) in to memory for Category-based Content Filtering application, and/or to load the rater.pkg file.

If the default directory of /cf does not exist on the flash, it will create the same. It also locates the recent full database and loads it into memory. This command also clears the old and excess incremental databases.

**Important:** This command is not supported on all platforms.

Example

The following command upgrades the SRDB for the Category-based Content Filtering application:

```
upgrade content-filtering category database
```
upgrade url-blacklisting database

This command upgrade the URL Blacklisting database.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

```
upgrade url-blacklisting database [ -noconfirm ]
```

- `noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to upgrade and load URL Blacklisting database whenever required.

Example

```
upgrade url-blacklisting database
```
Chapter 92
Exec Mode Show Commands (A-C)

This section includes the commands `show` through `show css service`.
The following commands provide outputs for a variety of parameters and statistics:
show aaa

Use this command to view AAA statistics for the current context.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show aaa { group { all | name aaa_group } | local counters } [ | { grep grep_options | more } ]

group { all | name aaa_group }
Displays AAA group configuration parameters.
all: If the exec context is local, all the default AAA groups, and the AAA groups configured in all the contexts are displayed. If the exec context is not local, only the context specific AAA groups are displayed.
name aaa_group: Displays AAA group configuration of the specified group. aaa_group must be the name of an existing AAA group, and must be a string of 0 to 64 characters in length.

local counters
Displays information for current context.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
This command is used to view accounting and authentication statistics for the current context.

Example
The following command displays AAA statistics for the current context:

show aaa local counters

The following command displays AAA statistics for the AAA group aaa_group1:

show aaa group name aaa_group1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging analyzer statistics

This command displays statistic information for protocol analyzers.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging analyzer statistics [ name protocol [ verbose ] ] [ | {
grep grep_options | more } ]

name protocol
Displays detailed information for the specified protocol analyzer.
protocol must be an available analyzer name, and must be one of the following:
• dns
• file-transfer
• ftp
• http
• icmp
• icmpv6
• imap
• ip
• ipv6
• mms
• p2p
• pop3
• pptp
• rtcp
• rtp
• rtp
• sdp
• secure-http
• sip
• smtp
• tcp
• tftp
• udp
"wsp
"wtp

verbose
Indicates the output should provide as much information as possible. If this option is not specified then the output is the standard level which is the concise mode.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display statistic information for active charging protocol analyzers.

Example
The following command displays detailed statistic information for all P2P protocol analyzers:

    show active-charging analyzer statistics name p2p verbose

The following command displays detailed statistic information for all TCP protocol analyzers:

    show active-charging analyzer statistics name tcp verbose

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging bandwidth-policy

This command displays information on bandwidth policies configured in a service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging bandwidth-policy { all | name bandwidth_policy } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all bandwidth policies configured in the service.

- **name**
  Displays detailed information for the specified bandwidth policy.
  `bandwidth_policy` must be a bandwidth policy name, and must be a string from 1 through 63 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view information on bandwidth policies configured in a service.

Example
The following command displays detailed information for the bandwidth policy named `standard`

```
show active-charging bandwidth-policy name standard
```
show active-charging charging-action

This command displays information for charging actions configured in the active charging service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging charging-action { { all | name action_name } [ service name ecs_service_name ] } | statistics [ name action_name ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for each configured charging action.

- **name action_name**
  Displays detailed information for specific charging action.
  `action_name` must be a string of 1 through 63 characters in length.

- **statistics**
  Displays statistical information for all configured charging action.

- **service name acs_service**
  Displays information for all or specified charging action(s) in the specified Active Charging Service.
  `acs_service` must be the name of an ACS and must be a string of 1 through 15 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to display information for charging actions configured in a service.

Example

The following command displays a detailed information for all charging actions:

```
show active-charging charging-action all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging charging-action
show active-charging content-filtering category policy-id

This command displays Content Filtering category policy definitions.

**Important**: This command is not available on StarOS 8.0 and earlier.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show active-charging content-filtering category policy-id { all | id policy_id } [ | { grep grep_options | more } ]
```

- **all**
  Displays definitions of all Content Filtering category policies.

- **id policy_id**
  Displays definitions of a specific Content Filtering category policy. 
  `policy_id` must be a CF policy ID, and must be an integer from 1 through 4294967295.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view Content-Filtering category definitions for a specific/all Policy IDs.

**Example**

The following command displays Content Filtering category definitions for policy ID 3:

```
show active-charging content-filtering category policy-id id 3
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging content-filtering category statistics

This command displays category-based content filtering statistics.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging content-filtering category statistics [ rulebase { name rulebase_name | all } ] [ verbose ] [ | { grep grep_options | more } ]
```

- **rulebase { name rulebase_name | all }**
  - Displays category-based content filtering statistics, optionally for a specific or all rulebase.
  - `rulebase_name` must be the name of an existing rulebase, and must be an alpha and/or numeric string of 1 through 63 characters in length.
  - `all`: Displays category-based content filtering statistics for each configured rulebase in the active charging service separately.

- **verbose**
  - Specifies that the output should provide as much information as possible. If this option is not specified then the output is the standard level, which is the concise mode.

- **grep grep_options | more**
  - Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  - For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view category-based content filtering statistics for a specific rulebase, or cumulative statistics for all rulebases in an active charging service.

Example

The following command displays category-based content filtering statistics for the rulebase named `consumer`:

```
show active-charging content-filtering category statistics rulebase name consumer
```

The following command displays cumulative category-based content filtering statistics for all rulebases in verbose mode:

```
show active-charging content-filtering category statistics verbose
```
Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging content-filtering server-group

This command displays information for Content Filtering Server Group (CFSG) configured in the service.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show active-charging content-filtering server-group [ statistics [ verbose ] ] [ name cfsg_name ] [ | { grep grep_options | more } ]
```

- **name cfsg_name**
  Displays detailed information for the specified Content Filtering Server Group.
  `cfsg_name` specifies the name of the configured Content Filtering Server Group, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **statistics**
  Displays statistical information for all configured Content Filtering Server Groups.

- **verbose**
  Specifies that the output provide as much information as possible. If this option is not specified then the output is at the standard level, which is the concise mode.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

Use this command to display information for Content Filtering Server Group configured in a service.

**Example**

The following command displays information for the CFSG named `test12`:

```
show active-charging content-filtering server-group name test12
```

The following command displays detailed information for all CFSG:

```
show active-charging content-filtering server-group statistics verbose
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show active-charging credit-control

This command displays statistics for Diameter/RADIUS prepaid credit control service in the Active Charging Service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging credit-control { statistics [ all | group group_name ] | session-states [ rulebase rulebase_name ] [ content-id content_id ] } [ | { grep grep_options | more } ]
```

```
statistics [ all | group group_name ]
```

Displays prepaid credit control statistics.
- `all`: Displays all available statistics.
- `group group_name`: Displays statistics for the specified credit control group. `group_name` must be the name of a credit control group, and must be an alpha and/or numeric string of 1 through 63 characters in length.

```
session-states [ rulebase rulebase_name ] [ content-id content_id ]
```

Displays prepaid CCA session status based on rulebase and/or content ID.
- `rulebase rulebase_name`: Displays the CCA session state counts for the specified rulebase.
  - `rulebase_name`: must be the name of a rulebase configured for credit control service, and must be an alpha and/or numeric string of 1 through 63 characters in length.
- `content-id content_id`: Displays CCA session state counts for the specified content ID.
  - `content_id`: must be the content ID of a credit control service, and must be an integer from 1 through 65535.

```
grep grep_options | more
```

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
- `grep`: For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view statistics for Diameter/RADIUS prepaid credit control service in an Active Charging Service.

Example

The following command shows active charging statistics of configured Diameter or RADIUS Credit control Application:

```
show active-charging credit-control statistics
```
Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging edr-format

This command displays information about EDR formats configured in an Active Charging Service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging edr-format [ statistics ] [ all | name edr_format_name] [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all EDR formats.

- **statistics**
  Displays statistics for all or the specified EDR format.
  If neither **all** nor **name** is specified, summarized statistics over all EDR formats is displayed.

- **name edr_format_name**
  Displays information for the specified EDR format.
  *edr_format_name* must be the name of an existing EDR format, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage
Use this command to display information for EDR format(s) in an active charging service.

Example
The following command displays all configured EDR formats in a active charging service.

```
show active-charging edr-format all
```

⚠️ **Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging edr-udr-file

This command displays CDR flow control information. This command also displays the EDR and UDR file related information.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging edr-udr-file { flow-control-counters [ verbose ] | statistics } [ | { grep grep_options | more } ]
```

```
flow-control-counters [ verbose ]
Displays the counters for dropped EDR/UDR records. These counters are for when CDRMOD uses flow control to stop ACSMgs/SessMgs from sending the records.
verbose displays detailed information.
```

```
statistics
Displays EDR and UDR file statistics.
```

```
grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
```

Usage
Use this command to view CDR flow control information.

Example
The following command displays EDR and UDR files statistics:

```
show active-charging edr-udr-file statistics
```

The following command displays CDR flow control information:

```
show active-charging edr-udr-file flow-control-counters
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging file-space-usage

This command displays the file space used by CDR/EDR files.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging file-space-usage [ | { grep grep_options | more } ]
```

**grep grep_options | more**

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view CDR/EDR file space usage information. The context in which this command is used is not relevant.
show active-charging firewall statistics

This command displays Active Charging Stateful Firewall statistics.

Product
- FW

Privilege
- Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging firewall statistics [ callid call_id | domain-name domain_name | nat-realm nat_realm | protocol { icmp | ip | other | tcp | udp } | username user_name ] [ acsmgr instance instance_id ] [ verbose ] [ | { grep grep_options | more } ]

- **acsmgr instance instance_id**
  Specifies an ACS/Sess Manager instance ID.
  - *instance_id* must be an integer from 1 through 65535.

- **callid call_id**
  Specifies a Call Identification number.
  - *call_id* must be an eight-digit HEX number.

- **domain-name domain_name**
  Specifies a domain name for the statistics.
  - *domain_name* must be a string of 1 through 127 characters in length.

- **nat-realm nat_realm**
  Specifies a NAT realm name for the statistics.
  - *nat_realm* must be a string of 1 through 31 characters in length.

- **protocol { icmp | ip | other | tcp | udp }**
  Specifies a protocol for the statistics:
  - **icmp**: ICMP protocol
  - **ip**: IP protocol
  - **other**: Protocols other than TCP, UDP, and ICMP
  - **tcp**: TCP protocol
  - **udp**: UDP protocol

- **username user_name**
  Specifies user name for the statistics.
  - *user_name* must be a string of 1 through 127 characters in length.
**verbose**
Specifies that the output should provide as much information as possible. If this option is not specified then the output is the standard level, which is the concise mode.

**grep grep_options | more**
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
Use this command to view Active Charging Stateful Firewall statistics. If you are in the local context, statistics for all contexts are displayed. Otherwise, only statistics of your current context are displayed.

**Example**
The following command displays Active Charging Stateful Firewall statistics:

```
show active-charging firewall statistics
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging firewall track-list

This command displays the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

**Product**
FW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```bash
show active-charging firewall track-list attacking-servers [ | { grep grep_options | more } ]
```

- `grep grep_options | more`

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view details of servers being tracked for involvement in any DOS attack.

**Example**

The following command displays the list of servers being tracked for involvement in any DOS attacks:

```bash
show active-charging firewall track-list attacking-servers
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging flows

This command displays information for active charging flows.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging flows { all | [ connected-time [ < | > | greater-than | less-than ] seconds ] [ flow-id flow_id ] [ full ] [ idle-time [ < | > | greater-than | less-than ] seconds ] [ ip-address [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] address ] [ nat { not-required | required [ nat-ip nat_ip_address ] } ] [ port-number [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] number ] [ rx-bytes [ < | > | greater-than | less-than ] number ] [ rx-packets [ < | > | greater-than | less-than ] number ] [ session-id session_id ] [ summary ] [ trans,proto { icmp | tcp | udp } ] [ tx-bytes [ < | > | greater-than | less-than ] number ] [ tx-packets [ < | > | greater-than | less-than ] number ] [ type flow_type ] } [ | { grep grep_options | more } ]

all
Displays information for all active charging flows.

connected-time [ < | > | greater-than | less-than ] seconds
Displays information for flows filtered by connected time period.
  •< seconds: Displays flows that have been connected less than the specified number of seconds.
  •>> seconds: Displays flows that have been connected more than the specified number of seconds.
  •greater-than seconds: Displays flows that have been connected more than the specified number of seconds.
  •less-than seconds: Displays flows that have been connected less than the specified number of seconds.

seconds must be an integer from 0 through 4294967295.

flow-id flow_id
Displays information for specified active charging flow ID.

full
Displays all available information for the specified flows.

idle-time [ < | > | greater-than | less-than ] seconds
Displays information for flows filtered by idle time period.
  •< seconds: Displays flows that have been idle less than the specified number of seconds.
  •>> seconds: Displays flows that have been idle more than the specified number of seconds.
show active-charge flows

• **greater-than seconds**: Displays flows that have been idle more than the specified number of seconds.
• **less-than seconds**: Displays flows that have been idle less than the specified number of seconds.

*seconds* must be an integer from 0 through 4294967295.

```plaintext
ip-address [ server | subscriber ][ < | > | IPv4 | greater-than | less-than ] address
```

Displays information for flows filtered by IPv4 IP address.

• **server**: Specifies the ip address for a specific server.
• **subscriber**: Specifies subscriber details for this *ip-address*. *address* is an IPv4 IP address in the *x.x.x.x* format.
• **< address**: Specifies an IPv4 IP address that is lesser than *address*.
• **> address**: Specifies an IPv4 IP address that is greater than *address*.
• **greater-than address**: Specifies an IPv4 IP address that is greater than *address*.
• **less-than address**: Specifies an IPv4 IP address that is lesser than *address*.

*address* must be an IPv4 address in decimal notation.

```plaintext
nat { not-required | required [ nat-ip nat_ip_address [ nat-port nat_port ] ] }
```

**Important**: The **nat** keyword and options are only available in StarOS 8.3 and later releases.

Displays information for flows filtered by Network Address Translation (NAT) required or not required setting.

• **not-required**: Sessions with NAT processing not required.
• **required**: Sessions with NAT processing required.
• **nat-ip nat_ip_address**: Sessions using specified NAT IP address. *nat_ip_address* must be an IPv4 address in dotted decimal format.
• **nat-port nat_port**: Sessions using specified NAT IP address and NAT port number. *nat_port* must be an integer from 0 through 65535.

```plaintext
port-number [ server | subscriber ][ < | > | IPv4 | greater-than | less-than ] number
```

Displays information on flows filtered by port number.

• **server**: Specifies the port-number for a specific server.
• **subscriber**: Specifies subscriber details for this *port-number*. *number* must be an integer from 0 through 65535.
• **< number**: Specifies a port number that is less than the specified *port-number*.
• **> number**: Specifies a port number that is greater than the specified *port-number*.
• **greater-than number**: Specifies a port number that is greater than the specified *port-number*.
• **less-than number**: Specifies a port number that is less than the specified *port-number*.
**rx-bytes [ < | > | greater-than | less-than ] number**

Displays information on flows filtered by the number of bytes received in the flow.
- `< number`: Specifies the number of bytes that is less than the specified `rx-bytes`.
- `> number`: Specifies number of bytes that is greater than the specified `rx-bytes`.
- `greater-than number`: Specifies number of bytes that is greater than the specified `rx-bytes`.
- `less-than number`: Specifies number of bytes that is less than the specified `rx-bytes`.

`number` must be an integer from 0 through 18446744073709551615.

**rx-packets [ < | > | greater-than | less-than ] number**

Displays information on flows filtered by the number of packets received in the flow.
- `greater-than number`: Specifies the number of packets that is greater than the specified `rx-packets`.
- `less-than number`: Specifies the number of packets that is less than the specified `rx-packets`.

`number` must be an integer from 0 through 18446744073709551615.

**session-id session_id**

Displays detailed information for specific active charging session ID.

**summary**

Displays summary information for defined sessions, based on defined parameters.

**trans-proto { icmp | tcp | udp }**

Displays information on flows filtered by the transport protocol.
- `icmp`: ICMP protocol type flow
- `tcp`: TCP protocol type flow
- `udp`: User Datagram Protocol (UDP) flows

**tx-bytes [ < | > | greater-than | less-than ] number**

Displays information on flows filtered by the number of bytes received in the flow.
- `< number`: Specifies the number of bytes that is less than the specified `tx-bytes`.
- `> number`: Specifies number of bytes that is greater than the specified `tx-bytes`.
- `greater-than number`: Specifies number of bytes that is greater than the specified `tx-bytes`.
- `less-than number`: Specifies number of bytes that is less than the specified `tx-bytes`.

`number` must be an integer from 0 through 18446744073709551615.

**tx-packets [ < | > | greater-than | less-than ] number**

Displays information on flows filtered by the number of packets received in the flow.
- `greater-than number`: Specifies the number of packets that is greater than the specified `tx-packets`.
- `less-than number`: Specifies the number of packets that is less than the specified `tx-packets`.

`number` must be an integer from 0 through 18446744073709551615.
**type flow_type**

Displays information on flows filtered by flow type of application protocol.

*flow_type* must be one of the following:

- `dns`
- `ftp`
- `http`
- `icmp`
- `icmpv6`
- `imap`
- `ip`
- `ipv6`
- `mms`
- `p2p`: P2P protocol type flows including one or more of the following applications:
  - `actsync`
  - `aimini`
  - `applejuice`
  - `ares`
  - `battlefd`
  - `bittorrent`
  - `ddlink`
  - `directconnect`
  - `edonkey`
  - `fasttrack`
  - `feidian`
  - `filetopia`
  - `freenet`
  - `fring`
  - `gadu_gadu`
  - `gnutella`
  - `gtalk`
  - `halflife2`
  - `hamachivpn`
  - `iax`
  - `imesh`
  - `iptv`
  - `iskoot`
  - `irc`
show active-charging flows

*jabber
*manolito
*msn
*mute
*nimbuzz
*ooovo
*openft
*orb
*oscar
*paltalk
*pando
*pandora
*popo
*pplive
*ppstream
*qq
*qqgame
*qqlive
*quake
*rdp
*secondlife
*skinny
*skype
*slingbox
*sopcast
*soulseek
*steam
*tvants
*tvuplayer
*uusee
*vpx
*vtun
*warcft3
*winmx
*winny
*wofwarcraft
*xbox
show active-charging flows

- yahoo
- zattoo
- pop3
- pptp
- rtp
- rtcp
- rtsp
- secure-http
- sip
- smtp
- tcp
- tftp
- udp
- unknown: Unknown type of protocol type flow not listed here.
- wsp-connection-less
- wsp-connection-oriented

**grep grep_options | more**

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.

For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

**Usage**

Use this command to display charging flow type information.

**Example**

The following command displays a detailed flow information for a session ID of `test`:

```
show active-charging flows session-id test
```

The following command displays a detailed flow information for a P2P type session:

```
show active-charging flows full type p2p
```

The following command displays a detailed information for a P2P type flow:

```
show active-charging flows type p2p
```

**Important:** Output descriptions for commands are available in the `Statistics and Counters Reference`.
show active-charging fw-and-nat policy

This command displays Firewall-and-NAT Policy information.

Important: This command is only available in StarOS 8.1, and in StarOS 9.0 and later. For more information on this command please contact your local service representative.

Product
ECS, FW, NAT

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging fw-and-nat policy { { { all | name fw_nat_policy } [ service name acs_service ] } | { statistics { all | name fw_nat_policy } } } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all Firewall-and-NAT policies configured, optionally all in a specified service.

- **name fw_nat_policy**
  Displays detailed information for the specified Firewall-and-NAT policy.
  
  `fw_nat_policy` specifies the Firewall-and-NAT policy name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **service name acs_service**
  Displays information for all or the specified Firewall-and-NAT policy in the specified Active Charging Service.
  
  `acs_service` must be the name of an Active Charging Service, and must be an alpha and/or numeric string of 1 through 15 characters in length.

- **statistics**
  Displays statistics for the all/specified Firewall-and-NAT policy.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view Firewall-and-NAT Policy information.
Example
The following command displays detailed information for the Firewall-and-NAT policy named `standard`:

```
show active-charging fw-and-nat policy name standard
```
show active-charging group-of-prefixed-urls

This command displays information on group of prefixed URLs configured in a service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show active-charging group-of-prefixed-urls { all | name prefixed_url_group } [ service name acs_service ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Displays information for all group of prefixed URLs configured in a service.</td>
</tr>
<tr>
<td><strong>name prefixed_url_group</strong></td>
<td>Displays detailed information for the specified group of prefixed URLs. prefixed_url_group must be the name of a group of prefixed URLs, and must be a string of 1 through 63 characters in length.</td>
</tr>
<tr>
<td><strong>service name acs_service</strong></td>
<td>Displays information for all or the specified group of prefixed URLs within the specified Active Charging Service. acs_service must be a string of 1 through 15 characters in length.</td>
</tr>
<tr>
<td>**grep grep_options</td>
<td>more**</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to view information on group of prefixed URLs configured in an Active Charging Service.

**Example**
The following command displays for the group of prefixed URLs named **test123**:

```
show active-charging group-of-prefixed-urls name test123
```
show active-charging group-of-ruledefs

This command displays information on group of ruledefs configured in a service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging group-of-ruledefs { { all | name group_of_ruledefs } [ service name acs_service ] | statistics name group_of_ruledefs } [ | { grep grep_options| more } ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Displays information for all groups of ruledefs configured, optionally all in a specified service.</td>
</tr>
<tr>
<td><strong>name group_of_ruledefs</strong></td>
<td>Displays detailed information for the specified group of ruledefs. <code>group_of_ruledefs</code> must be the name of a group of ruledefs, and must be a string of 1 through 63 characters in length.</td>
</tr>
<tr>
<td><strong>service name acs_service</strong></td>
<td>Displays information for all or the specified group of ruledefs within the specified Active Charging Service. <code>acs_service</code> must be the name of an Active Charging Service, and must be a string of 1 through 15 characters in length.</td>
</tr>
<tr>
<td><strong>statistics name group_of_ruledefs</strong></td>
<td>Displays statistics for the specified group of ruledefs. <code>group_of_ruledefs</code> must be the name of a group of ruledefs, and must be a string of 1 through 63 characters in length.</td>
</tr>
<tr>
<td>**grep grep_options</td>
<td>more**</td>
</tr>
</tbody>
</table>

Usage
Use this command to view information on group of ruledefs configured in a service.

Example
The following command displays information on all groups of ruledefs configured:

```
show active-charging group-of-ruledefs all
```
show active-charging group-of-ruledefs
show active-charging nat statistics

This command displays NAT realm statistics.

Product
NAT

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging nat statistics [ nat-realm nat_realm [ summary ] ] [ | {
grep grep_options | more } ]

Usage
Use this command to view NAT realm statistics.

Example

This command when issued in the local context displays statistics for all NAT realms in all contexts. When issued in a specific context, this command displays statistics for all NAT realms in that context.

show active-charging nat statistics nat-realm nat_realm

This command when issued in the local context displays statistics for the specified NAT realm in all contexts. When issued in a specific context, this command displays statistics for the specified NAT realm in that context.

nat-realm nat_realm

Specifies the NAT realm’s / NAT realm group’s name.
nat_realm must be an alpha and/or numeric string of 1 through 31 characters in length.

summary

When the nat_realm specified is a “pool group” and the summary option is used, summary statistics of all pools in the pool group is displayed.
When the nat_realm specified is a pool and the summary option is NOT used, all available statistics for the specified pool is displayed.
When the nat_realm specified is a “pool group” and the summary option is NOT used, all available statistics of each pool in the specified “pool group” is displayed.

grep grep_options | more

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
The following command when issued in the local context, displays NAT realm statistics for NAT realms named *test135* in all contexts:

```
show active-charging nat statistics nat-realm test135
```
show active-charging p2p-dynamic-rules

This command displays P2P Dynamic signature file information.

Product
P2P

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging p2p-dynamic-rules [ verbose ] [ acsmgr instance instance_id ] [ | { grep grep_options | more } ]
```

```
acsMgr instance instance_id

Specifies an ACS Manager instance ID.
instance_id must be an integer from 1 through 65535.
```

```
verbose

Displays P2P Dynamic rule statistics in detail.
```

```
grep grep_options | more

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
```

Usage

Use this command to view P2P Dynamic signature file statistics/information.

Example

The following command displays P2P Dynamic rule information:

```
show active-charging p2p-dynamic-rules
```
show active-charging packet-filter

This command displays information on packet filters configured in a service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show active-charging packet-filter { all | name packet_filter } [ service name acs_service ] [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all packet filters configured, optionally all configured in a service.

- **name packet_filter**
  Displays detailed information for the specified packet filter.
  `packet_filter` must be a packet filter’s name, and must be a string of 1 through 63 characters in length.

- **service name acs_service**
  Displays information for all or the specified packet filter within the specified Active Charging Service.
  `acs_service` must be the Active Charging Service’s name, and must be a string of 1 through 15 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view information on packet filters configured in a service.

**Example**

The following command displays information for the packet filter `filter12`:

```
show active-charging packet-filter name filter12
```
show active-charging rulebase

This command shows information for rulebases configured in a system or service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging rulebase { { all | name rulebase_name } [ service name acs_service ] } | statistics [ name rulebase_name ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays details of all rulebases configured in the system.

- **name rulebase_name**
  Displays details of the specified rulebase.
  `rulebase_name` must be string of 1 through 63 characters in length.

- **service name acs_service**
  Displays details of all or the specified rulebase configured within the specified Active Charging Service.
  `acs_service` must be a string of 1 through 15 characters in length.

- **statistics**
  Displays statistical information for all or the a specific rulebase.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view various statistics for a specific charging rulebase.

Example

The following command displays active charging rulebase statistics.

```
show active-charging rulebase statistics
```

The following command displays configurations and statistics for a Rulebase named `rulebase_1`.

```
show active-charging rulebase name rulebase_1
```
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging ruledef

This command displays information for rule definitions (ruledefs) configured in the ACS service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging ruledef { all | charging | firewall | name ruledef_name | post-processing | routing | statistics [ all { charging | firewall [ wide ] | post-processing } | name ruledef_name [ wide ] ] ] [ | { grep grep_options | more } ]
```

all
Displays information for all ruledefs configured in the ACS service.

charging
Displays information for all Charging ruledefs configured in the ACS service.

firewall
Displays information for all Firewall ruledefs configured in the ACS service.

name ruledef_name
Displays detailed information for the specified ruledef. ruledef_name must be the name of an existing ruledef, and must be a string of 1 through 63 characters in length.

post-processing

**Important:** This keyword is only available in StarOS 8.3 and later.

Displays information for all post-processing ruledefs configured in the ACS service.

routing
Displays information for all Routing ruledefs configured in the ACS service.

service svc_name
This keyword is obsolete.

statistics [ all { charging | firewall [ wide ] | post-processing } | name ruledef_name [ wide ] ]
Displays statistical information for all/specified ruledefs configured in the ACS service. If none of the optional arguments are supplied, statistics totaled for all ruledefs will be displayed.
show active-charging ruledef

**all**: Displays statistics for all ruledefs of the specified type configured in the ACS service.
**charging**: Displays statistics for all Charging ruledefs configured in the service.
**firewall**: Displays statistics for all Firewall ruledefs configured in the service.
**post-processing**: Displays statistics for all Post-processing ruledefs configured in the service.

---

**Important**: The post-processing keyword is only available in StarOS 8.3 and later.

**name ruledef_name**: Displays statistics for the specified ruledef. *ruledef_name* must be the name of an existing ruledef, and must be a string of 1 through 63 characters in length.
**wide**: Displays all available information in a single wide line.

---

**grep grep_options | more**

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

**Usage**

Use this command to view information for ruledefs configured in the ACS service.

---

**Example**
The following command displays active charging ruledef statistics.

```
show active-charging ruledef statistics
```

---

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging service

This command displays Active Charging Service details.

**Product**

ECS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show active-charging service { all | name acs_service } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all configured Active Charging Service.

- **name acs_service**
  Displays detailed information for the specified Active Charging Service.
  `acs_service` must be a string of 1 through 15 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view Active Charging Service details.

**Example**

The following command displays details for the Active Charging Service named `test1`.

```
show active-charging service name test1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging sessions

This command displays statistics for Active Charging Service sessions.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging sessions [ full [ wide ] | summary | display-dynamic-charging-rules | dynamic-charging ] { [ all ] | [ filter_keyword ] + } [ | { grep grep_options | more } ]

- **full [ wide ]**
  Displays all available information for the specified session. Optionally all available information can be displayed in a single wide line.

- **summary**
  Displays summary information for defined sessions based on defined parameters.

- **display-dynamic-charging-rules**
  Displays information for the dynamic-charging rules configured per session under Gx/Ty interface support.

- **dynamic-charging**
  Displays information for dynamic charging sessions.

- **filter_keyword**
  The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all command keywords. Multiple filter keywords can be entered on a command line. When multiple filter keywords are specified, the output conforms to all of the filter keywords specifications. For example, if you enter the following command:

  ```
  show active-charging sessions full active-charging-service acs_1
  ```

  Counters for active charging sessions active in active charging service `acs_1` with full details is displayed. Information for all other services is not displayed.

- **acsmgr instance instance**
  Displays session information for a specific ACS/Sess Manager instance.

- **active-charging-service acs_service**
  Displays session information for the specified Active Charging Service.

- **all**
  Displays session information for all active charging sessions.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>callid</code></td>
<td>Specifies the call identification number.</td>
</tr>
<tr>
<td><code>display-dynamic-charging-rules</code></td>
<td>Displays Dynamic Charging Rules configured.</td>
</tr>
<tr>
<td><code>dynamic-charging</code></td>
<td>Displays session information for all Dynamic Charging Sessions.</td>
</tr>
<tr>
<td>`firewall { not-required</td>
<td>required }`</td>
</tr>
<tr>
<td><code>fw-and-nat policy fw_nat_policy</code></td>
<td>Displays information for the specified Firewall-and-NAT Policy.</td>
</tr>
<tr>
<td></td>
<td><em>fw_nat_policy</em> specifies the Firewall-and-NAT policy name, and must be an alpha and/or numeric string of 1 through 63 characters in length.</td>
</tr>
<tr>
<td><code>imsi</code></td>
<td>Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>Specifies the IP address for the specific charging service.</td>
</tr>
<tr>
<td><code>msid</code></td>
<td>Displays active charging session information for a specific subscriber’s Mobile Station Identification (MSID) number.</td>
</tr>
<tr>
<td>`nat { not-required</td>
<td>required [ nat-realm nat.realm ] }`</td>
</tr>
<tr>
<td></td>
<td><em>nat-realm nat.realm</em> specifies a NAT realm name. <em>nat.realm</em> must be a string from 1 through 63 characters in length.</td>
</tr>
<tr>
<td><code>rulebase</code></td>
<td>Displays information for a rulebase that is configured in an active charging session.</td>
</tr>
<tr>
<td><code>rx-data</code></td>
<td>Displays the bytes received in the session.</td>
</tr>
<tr>
<td><code>session-id</code></td>
<td>Displays detailed session information for a specific session identification.</td>
</tr>
<tr>
<td><code>tx-data</code></td>
<td>Displays the bytes sent in the session.</td>
</tr>
</tbody>
</table>
show active-charging sessions

type
Displays session information for specified DNS application type(s).
  • dns
  • ftp
  • http
  • icmp
  • icmpv6
  • imap
  • ip
  • ipv6
  • mms
  • p2p: Displays session information for a P2P application type:
    • actsync
    • aimini
    • applejuice
    • ares
    • battlefd
    • bittorrent
    • dmlink
    • directconnect
    • edonkey
    • fasttrack
    • feidian
    • filetopia
    • freenet
    • fring
    • gadu_gadu
    • gnutella
    • gtalk
    • halflife2
    • hamachivpn
    • iax
    • imesh
    • irc
    • iskoot
    • jabber
    • manolito
• msn
• mute
• nimbuzz
• oovoo
• openft
• orb
• oscar
• paltalk
• pando
• pandora
• popo
• pplive
• ppstream
• qq
• qqgame
• qqlive
• quake
• rdp
• secondlife
• skinny
• skype
• slingbox
• sopcast
• soulseek
• steam
• tvants
• tvuplayer
• uusee
• vpnx
• vtun
• warcft3
• winmx
• winny
• wofwarcraft
• xbox
• yahoo
• zattoo
show active-charging sessions

*pop3
*pptp
*rtcp
*rtp
*rtsp
*secure-http
*sip
*smtp
/tcp
*tftp
*udp
*unknown
*wsp-connection-less
*wsp-connection-oriented

username
Displays session information for a specific user name.

dynamic-charging
Displays the all sessions having received at least one Gx message from Session Manager/IMS Authorization.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display the configuration information for an active charging session.

Example
The following command displays full information of an active charging session.

    show active-charging sessions full all

The following command displays an active charging session summary.

    show active-charging sessions summary

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging subsystem

This command shows service and configuration counters for the active charging service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging subsystem { all | facility acsmgr { all | instance instance_value } } [ rulebase name rulebase_name ] | [ | { grep grep_options | more } ]
```

- **all**
  Displays active charging service subsystem information.

- **facility acsmgr { all | instance instance_value }**
  Displays logged events for all active charging managers or for a specific instance. `instance_value` must be an integer from 1 through 65535.

- **rulebase name rulebase_name**
  Displays rulebase statistics for a specific rulebase configured in a system.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to display information for active charging service manager.

Example

The following command displays active charging service subsystem information.

```
show active-charging subsystem all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging timedef

This command displays the details of timeslots configured in specified time definition(s).

**Important:** This command is only available in StarOS 8.1 and in StarOS 9.0 and later.

**Product**
ECS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```plaintext
show active-charging timedef { all | name timedef_name } [ service name acs_service ] [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all timedefs configured in the service.

- **name timedef_name**
  Displays detailed information for the specified timedef.
  `timedef_name` must be the name of a timedef, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **service name acs_service**
  Displays information for all or a specific timedef configured within the specified Active Charging Service.
  `acs_service` must be the Active Charging Service name, and must be an alpha and/or numeric string of 1 through 15 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

Use this command to view details of timeslots configured in specified timedef(s) that have been configured for the Time-of-Day Activation/Deactivation of Rules feature.

**Example**
The following command displays timeslot details of all timedefs configured in the Active Charging Service:

```plaintext
show active-charging timedef all
```
show active-charging timedef
show active-charging udr-format

This command displays information about UDR formats configured in an Active Charging Service.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging udr-format { all | name udr_format_name } [ | { grep grep_options | more } ]
```

- `all`
  Displays information for all UDR formats.

- `name udr_format_name`
  Displays information for the specified UDR format.
  `udr_format_name` must be the name of an existing UDR format, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- `grep grep_options | more`
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the `Regulating a Command's Output` section of the `Command Line Interface Overview` chapter in the `Command Line Interface Reference`.

Usage
Use this command to display information for UDR format(s) in an active charging service.

Example
The following command displays all configured UDR formats in a active charging service.

```
show active-charging udr-format all
```

**Important**: Output descriptions for commands are available in the `Statistics and Counters Reference`.
show active-charging url-blacklisting statistics

This command displays URL Blacklisting statistics.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show active-charging url-blacklisting statistics [ rulebase { all | name rulebase_name } ] [ verbose ] [ | { grep grep_options | more } ]
```

- **rulebase { all | name rulebase_name }**
  Displays information on URL Blacklisting configured in a rulebase.
  - **all**: Displays URL Blacklisting statistics for all rulebases.
  - **name rulebase_name**: Displays URL Blacklisting statistics for the specified rulebase. `rulebase_name` must be a rulebase name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

- **verbose**
  Displays detailed URL Blacklisting statistics.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

Use this command to view URL Blacklisting hits and misses statistics.

**Example**

The following command displays cumulative URL Blacklisting statistics:

```
show active-charging url-blacklisting statistics
```

The following command displays URL Blacklisting statistics for the rulebase `rulebase_1`:

```
show active-charging url-blacklisting statistics rulebase name rulebase_1
```

**Important**: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging xheader-format

This command displays x-header format configurations.

Important: This is a customer-specific command. Please contact your local sales representative for more information.

Product
ECS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show active-charging xheader-format { all | name xheader_format } [ | { grep grep_options | more } ]

all
Displays information for all x-header formats configured.

ame xheader_format
Displays information for the specified x-header format.
xheader_format must be an x-header format’s name, and must be a string of 1 through 63 characters in length.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view details of x-header formats configured in a service.

Example
The following command displays information for the x-header format named test12:

show active-charging xheader-format test12
show administrators

Displays information regarding all CLI users currently connected to the system.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show administrators [ session id ] [ | { grep grep_options | more } ]
```

- **session id**
  Indicates the output is to contain additional information about the CLI user session including the assigned session ID.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

This command displays a list of administrative users that have command line interface sessions active.

Example

```
show administrators
show administrators session id
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show alarm

Displays alarm information.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
showalarm { all | audible | central-office | facility | outstanding [ all | chassis | port slot/port | slot slot ] [ verbose ] | statistics } [ | { grep grep_options | more } ]
```

- **all**
  Displays the state of all alarms in one screen.

- **audible**
  Displays the state of the internal audible alarm buzzer on the SMC.

- **central-office**
  Displays the state of the CO Alarm relays on the SPIO.

- **facility**
  Displays the state of the facility (audible and CO) alarms.

- **outstanding [ all | chassis | port slot/port | slot slot ] [ verbose ]**
  Displays information on currently outstanding alarms.
  - **all**: Displays all alarm information.
  - **chassis**: Displays chassis/power/fan alarms.
  - **port slot/port**: Shows the alarm information for the specified port.
  - **slot slot**: Shows the alarm information for the card in the specified slot.
  - **verbose**: Displays more verbose output, including the internal alarm ID

- **statistics**
  Displays basic statistics on the alarming subsystem, including the current number of outstanding alarms of different severities and a cumulative total of alarms generated.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
**Usage**

View alarms to verify system status or to periodically check the general health of the system.

**Important:** This command is not supported on all platforms.

**Example**

The following command displays all alarms that are currently outstanding:

```
show alarm outstanding all
```

The following command displays more detailed information on all alarms that are currently outstanding:

```
show alarm outstanding all verbose
```

The following command displays alarm statistics:

```
show alarm statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show apn

Displays configuration information for either a specific or all configured APNs.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show apn { all | name apn_name } [ | { grep grep_options | more } ]
```

```
all
Displays information on all APNs configured on the system.
```

```
name apn_name
Displays information for a specific APN.
apn_name is the name of the APN and can be from 1 to 62 alpha and/or numeric characters and is case sensitive.
```

```
grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more options, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
```

Usage
This command is used to verify the configuration of one or all APNs for monitoring or troubleshooting purposes. The output is a concise listing of APN parameter settings.
If this command is executed from within the local context with the all keyword, information for all APNs configured on the system will be displayed.

Example
The following command displays configuration information for all APNs:

```
show apn all
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show apn counter ip-allocation

This command displays the IP allocation method information/statistics counters on per apn basis for all currently active calls.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show apn counter ip-allocation [all | name apn_name] [{grep grep_options | more}]

all
Displays statistics for all APNs.

name apn_name
Displays statistics for a specific APN. apn_name is the name of the preconfigured APN and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

{grep grep_options | more}
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
This command is used to display the IP allocation counters on per apn basis for all currently active calls. Output of this command gives the user clear idea of how many sessions in each apn are using a particular type of ip-allocation method.
If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example
The following command displays statistics for all APN on a system:

show apn counter ip-allocation all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show apn statistics

Displays APN statistics for either a specific or all configured APNs.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show apn statistics [ all | name apn_name ] [ | { grep grep_options | more } ]
```

- **all**
  Displays statistics for all APNs.

- **name apn_name**
  Displays statistics for a specific APN.
  *apn_name* is the name of the APN and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of *grep* and *more*, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

This command is used to view statistics for one or all APNs within a context for monitoring or troubleshooting purposes.
If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example

The following command displays statistics for an APN called isp2:

```
show apn statistics name isp2
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show asngw-service

This command displays information about selected Access Service Network Gateway (ASN GW) calls/services.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service { all | name service_name | session | statistics } [ bs-status [ address ip_addr | filter { all | icmp-monitored | no-calls | summary | up } ] [ ] [ grep grep_options | more ] ]

---

all
Displays information for all configured ASN GW services.

name service_name
Displays information only for the specified ASN GW service.
 service_name must be the name of an existing ASN GW service in the current context. The service name must be an alpha and/or numeric string of 1 through 63 characters in length.

session
Displays information about configured ASNGW sessions. See the show asngw-service session command

statistics
Total of collected information for specific protocol since last restart or clear command.

bs-status { address ip_addr | filter { all | icmp-monitored | no-calls | summary | up } }
Displays the ASN BS status based on IP address and various filters.
 address ip_addr specifies the IP address of ASN base station whose status is requested. ip_addr must be an IPv4 or IPv6 IP address of ASN BS.
 filter { all | icmp-monitored | no-calls | summary | up }: Filters the requested BS’s staus on the basis of following criteria:
  • all: Displays the status of all ASN BS.
  • icmp-monitored: Displays the status of ASN BS which are monitored through ICMP ping messages.
  • no-calls: Displays the status of ASN BS which has no active calls.
  • summary: Displays the summary of status of requested ASN BSs.
  • up: Displays the status of ASN BSs which are in active state.
show asngw-service

| { grep grep_options | more }

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view information for selected configured ASN GW services.

Example

The following command displays available information for all active ASN GW services.

```
show asngw-service all
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show asngw-service session

This command displays statistics for specific Access Service Network Gateway sessions.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show asngw-service session [ all | anchor-only [ full ] | callid call_id | counters | full | ip-address ipv4_address | msid msid_number | non-anchor-only [ full ] | peer-address ipv4_address | summary | username user_name ] [ | { grep grep_options | more } ]

**all**
Displays all related information for all active ASN GW service sessions.

**anchor-only**
Displays all available information for all active ASN GW service sessions on an anchor ASN GW only.

**callid call_id**
Displays available information for the specific call identification number. call_id must be an eight-digit HEX number.

**full**
Displays all available information for the associated display or filter keyword.

**ip-address ipv4_address**
IP address of the subscriber. ipv4_address must be an IPv4 address, in dotted decimal notation.

**msid msid_number**
Displays available information for the specific mobile station identification number. msid_number must be an MSID number.

**non-anchor-only**
Displays all available information for all active ASN GW service sessions on a non-anchor ASN GW only.

**peer-address ipv4_address**
Address of specific IP peer. ipv4_address must be an IPv4 address, in dotted decimal notation.

**summary**
Displays summary of available information for associated display or filter keyword (previous keyword).
**username user_name**

Name of specific user within current context. Displays available information for the specific user name. user_name must be followed by an user name. The user name can an alpha and/or numeric string of 1 through 127 characters in length.

```
| { grep grep_options | more }
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view configuration information for an ASN GW session.

**Example**

The following command displays all available ASN GW sessions.

```
show asngw-service session all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show asngw-service session counters

This command displays statistics for specific Access Service Network Gateway sessions.

**Product**
ASN GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**
```
show asngw-service session counters [ [ function-type { auth-relay | context-transfer | data-path | handoff | im-operation | ms-state-change | paging | qos } ] | [ anchor-only | callid call_id | ip-address ipv4_address | msid msid_number |
   non-anchor-only | peer-address ipv4_address | username user_name ] | [ r4-only | r6-only | verbose ] ] [ | ( grep grep_options | more ) ]
```

**anchor-only**
Displays all available information for all active anchor sessions in an ASN GW service.

**callid call_id**
Displays available information for the specific call identification number. 
*call_id* must be an eight-digit HEX number.

**function-type { auth-relay | context-transfer | data-path | handoff | im-operation | ms-state-change | paging | qos }**
Displays the counters for specific type of functions in an ASN GW session.

- **auth-relay**: Displays information about authentication relay messages.
- **context-transfer**: Displays information about context-transfer messages.
- **data-path**: Displays information about data-path registration messages.
- **handoff**: Displays information about hand-off messages.
- **im-operation**: Displays information about idle mode state operation messages.
- **ms-state-change**: Displays information about MS state change messages.
- **paging**: Displays information about paging messages.
- **qos**: Displays information about RR messages.

**ip-address ipv4_address**
IP address of the subscriber.
*ipv4_address* must be an IPv4 address, in dotted decimal notation.

**msid msid_number**
Displays available information for the specific mobile station identification number.
*msid_number* must be an MSID number.

**non-anchor-only**
Displays all available information for all active non-anchor sessions in an ASN GW service.
**show asngw-service session counters**

*peer-address ipv4_address*
Address of specific IP peer.
*ipv4_address* must be an IPv4 address, in dotted decimal notation.

*rx-only*
Displays all available counters for R6 interface in an ASN GW session.

*rx-only*
Displays all available counters for R4 interface in an ASN GW session.

*username user_name*
Displays available session information for the specific WiMAX user in ASN GW service session.
*user_name* must be followed by an user name.
The user name can an alpha and/or numeric string of 1 through 127 characters in length.

*verbose*
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

```
| { grep grep_options | more }
```
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**
Use this command to view the counters of an ASN GW session.

**Example**
The following command displays the counters for data path type function.

```
show asngw-service session counters function-type data-path
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

show asngw-service statistics

Displays statistics for all ASN GW sessions.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service statistics { [ function-type ( auth-relay | context-transfer | data-path | handoff | im-operations | ms-state-change | paging | qos | r4-only | r6-only ) ] | name service_name | r4-only | r6-only | verbose | peer-address ipv4_address [ verbose ] } [ | { grep grep_options | more } ]

function-type
Displays information about selected function type on R4 or R6 interface.

function-type ( auth-relay | context-transfer | data-path | handoff | im-operations | ms-state-change | paging | qos | r4-only | r6-only )
Displays the counters for specific type of functions in an ASN GW session.
auth-relay: Displays information about authentication relay messages.
context-transfer: Displays information about context-transfer messages.
data-path: Displays information about data-path registration messages.
handoff: Displays information about hand-off messages.
im-operations: Displays information about idle mode state operation messages.
ms-state-change: Displays information about MS state change messages.
paging: Displays information about paging messages.
qos: Displays information about RR messages.
r4-only: Displays information about selected function on R4 interface.
r6-only: Displays information about selected function on R6 interface.

name service_name
Displays specific service.
service_name must be a service name.
The service name can be one to 63 alpha and/or numeric characters long.

r4-only
Displays statistics of R4 interface in ASN GW services.

r6-only
Displays statistics of R6 interface in ASN GW services.

peer-address ipv4_address
Address of specific IP Peer.
ipv4_address must be an IPv4 address, in dotted decimal notation.
**show asngw-service statistics**

**verbose**
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

```
| { grep grep_options | more }
```
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
Use this command to display ASN GW statistics.

**Example**
The following command displays information about selected MS-State-Change function.

```
show asngw-service statistics function-type ms-state-change
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show asnpc-service

This command displays information about selected Access Service Network Paging Controller and Location Registry (ASN PC/LR) services.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show asnpc-service { all | id | name service_name | session | statistics } [ | { grep grep_options | more } ]
```

**all**
Displays information for all configured ASN PC services.

**paging-group**
Displays all the configured paging-groups and associated paging nodes, and the offset count. For a specific paging group, enter the paging group id number.

**name service_name**
Displays information only for the specified ASN PC service. `service_name` must be the name of an existing ASN PC service in the current context. The service name must be an alpha and/or numeric string of 1 through 63 characters in length.

**session**
Displays information about configured ASN PC sessions.

**statistics**
Total of collected information for specific protocol since last restart or clear command.

```
| { grep grep_options | more }
```
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view information for selected configured ASN PC services.

Example
The following command displays available information for all active ASN PC services.
show asnpc-service

show asnpc-service all

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show asnpc-service session

This command displays statistics for specific ASN PC service sessions.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show asnpc-service session [ all | callid call_id | counters | full | msid msid_number | peer-address ipv4_address | summary ] [ | { grep grep_options | more } ]
```

**all**
Displays all related information for all active ASN PC service sessions.

**callid call_id**
Displays available information for the specific call identification number.
*call_id* must be an eight-digit HEX number.

**full**
Displays all available information for the associated display or filter keyword.

**msid msid_number**
Displays available information for the specific mobile station identification number.
*msid_number* must be an MSID number.

**peer-address ipv4_address**
Address of specific peer.
*ipv4_address* must be an IPv4 address, in dotted decimal notation.

**summary**
Displays summary of available information for associated display or filter keyword (previous keyword).

**| { grep grep_options | more }**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage
Use this command to view configuration information for an ASN PC session.
Example
The following command displays all available ASN PC session counters in verbose mode.

```
show asnpc-service session all
```

The following command displays full ASN PC session counters in verbose mode.

```
show asnpc-service session full
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show asnpc-service session counters

This command displays session counters for ASN PC service sessions.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service session counters [ all | callid call_id | msid msid_number | peer-address ipv4_address | verbose ] [ | { grep grep_options | more } ]

all
Displays all available counters for all ASN PC service sessions.

callid call_id
Displays available information for the specific call identification number.
call_id must be an eight-digit HEX number.

msid msid_number
Displays available information for the specific mobile station identification number.
msid_number must be an MSID number.

peer-address ipv4_address
Address of specific IP peer.
ipv4_address must be an IPv4 address, in dotted decimal notation.

verbose
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep grep_options | more }
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view the counters of an ASN PC session.

Example
The following command displays the counters for ASN PC service sessions in verbose mode.
show asnpc-service session counters verbose

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show asnpc-service session counters verbose

This command displays session counters for ASN PC service sessions in complete detail.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show asnpc-service session counters verbose [ function-type { context-transfer | im-operations | ms-state-change | paging } ] [ all | callid call_id | msid msid_number | peer-address ipv4_address ] ] [ | { grep grep_options | more } ]
```

- **all**
  Displays all available counters for all ASN PC service sessions in verbose mode.

- **callid call_id**
  Displays available information for the specific call identification number in verbose mode. 
  *call_id* must be an eight-digit HEX number.

- **function-type { context-transfer | im-operations | ms-state-change | paging }**
  Displays the counters for specific type of functions in an ASN GW session.
  - **context-transfer**: Displays information about context-transfer messages.
  - **im-operations**: Displays information about idle mode state operation messages.
  - **ms-state-change**: Displays information about MS state change messages.
  - **paging**: Displays information about paging messages.

- **msid msid_number**
  Displays available information for the specific mobile station identification number in verbose mode. 
  *msid_number* must be an MSID number.

- **peer-address ipv4_address**
  Address of specific IP peer. 
  *ipv4_address* must be an IPv4 address, in dotted decimal notation.

- **r4-only**
  Displays statistics of R4 interface in ASN PC services in verbose mode.

- **r6-only**
  Displays statistics of R6 interface in ASN PC services in verbose mode.
show asnpc-service session counters verbose

Usage

Use this command to view the counters of an ASN PC session in verbose mode.

Example

The following command displays the counters for data path type function.

```
show asnpc-service session counters verbose
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*.
show asnpc-service statistics

Displays statistics for all ASN PC service sessions.

Product
ASN GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service statistics [ name service_name | peer-address ipv4_address | verbose ] [ | { grep grep_options | more } ]

name service_name
Displays specific service.
service_name must be a service name.
The service name can be one to 63 alpha and/or numeric characters long.

peer-address ipv4_address
Address of specific IP Peer.
ipv4_address must be an IPv4 address, in dotted decimal notation.

verbose
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep grep_options | more }
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to display ASN PC statistics.

Example
The following command displays information about ASN PC service in verbose mode.

show asnpc-service statistics verbose

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show asnpc-service statistics verbose

Displays statistics for all ASN PC service in verbose mode.

**Product**
ASN GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show asnpc-service statistics verbose [ function-type { context-transfer | im-operations | ms-state-change | paging } ] | all | r4-only | r6-only ] [ | { grep grep_options | more } ]
```

- **function-type**: Displays the statistics for specific type of functions in an ASN PC service in verbose mode.
  - `context-transfer`: Displays information about context-transfer messages.
  - `im-operations`: Displays information about idle mode state operation messages.
  - `ms-state-change`: Displays information about MS state change messages.
  - `paging`: Displays information about paging messages.

- **all**: Displays statistics of all ASN PC services in verbose mode.

- **r4-only**: Displays statistics of R4 interface in ASN PC services.

- **r6-only**: Displays statistics of R6 interface in ASN PC services.

| { grep grep_options | more } |

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to display ASN PC service statistics in verbose mode.

**Example**
The following command displays information about selected MS-State-Change function.

```
show asnpc-service statistics verbose function-type ms-state-change
```
show asnp-service statistics verbose

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show banner

Displays the configured banner message for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show banner { all | charging-service | motd | lawful-intercept | pre-login } [ | { grep grep_options | more } ]
```

- **all**
  Displays all banners configured for a service in a system including enhanced charging service.

- **charging-service**
  Displays banner message configured for a enhanced charging service in current context.

- **motd**
  Display the banner message that is configured for the current context.

- **lawful-intercept**
  Display the banner message that is configured for users that have Lawful Intercept privileges.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Show the configured banner to verify the message of the day contents for possible change

**Example**

```
show banner
```

---

*Cisco ASR 5000 Series Command Line Interface Reference*
show bcmcs counters

Displays BCMCS-specific counters and statistics.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show bcmcs counters { all | callid call_id | flow-id flow_id }
```

- **all**
  Displays BCMCS-specific counters and statistics for all multicast sessions.

- **callid call_id**
  Displays BCMCS-specific counters and statistics for a specific call ID.

- **flow-id flow_id**
  Displays BCMCS-specific counters and statistics for a specific BCMCS flow, defined by a flow ID.

Usage

Use this command to view BCMCS-specific statistics. You may narrow the results of the command output by specifying a specific call ID or flow ID.

Example

```
show bcmcs counters all
```

⚠️ **Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show bcmcs statistics

Displays BCMCS-specific statistics for the current PDSN-service.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show bcmcs statistics [ pdsn-service service_name]
```

**Usage**

Shows several sets of BCMCS-specific statistics, and may be configured to show statistics only for a certain PDSN service.

**Example**

```
show bcmcs statistics pdsn-service service_name
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show boot

Displays information on the current boot image in use.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show boot [ initial-config| { grep grep_options | more } ]
```

**initial-config**
Identifies the OS image, configuration file, and boot priority used during the initial start up of the system.

**grep grep_options | more**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Show the boot information in preparing for maintenance activities by verifying current boot data. The boot image in use may not be the same as the boot image stored on the SMC due to upgrades and pending reboots. `show boot initial-config` displays the actual boot image and configuration file loaded during boot. This may or may not be the highest priority image and makes this command useful when comparing the loaded image to the priority list.

**Important:** This command is not supported on all platforms.

Example
The following command displays the boot system configuration priority list:

```
show boot
```

The following command displays the initial configuration after a system boot:

```
show boot initial-config
```
show bssap+ statistics

Displays statistics for base station system application part plus in a Gs service sessions.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show bssap+ statistics [ gs-service gs_svc_name ] [ vlr { name vlr_name | isdn-number E164_ISDN_Num } ] [ verbose ] [ | { grep grep_options | more } ]
```

**gs-service gs_svc_name**
Specifies the name of a specific Gs service to filter the BSSAP+ information.

*gs_svc_name* is the name of a configured Gs service for which BSSAP+ is applied and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**vlr { name vlr_name | isdn-number E164_ISDN_Num }**
Specifies the name of the VLR or SS7 address in E.164 ISDN format to filter the BSSAP+ information.

*vlr_name* is name of the VLR must be an alpha and/or numeric string of 1 to 63 characters.

*E164_VLR_num* is an ISDN number for VLR per E.164 number plan and must be an numerical string of 1 to 15 digits.

**verbose**
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| {grep grep_options | more}

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
Use this command to display the statistics of BSSAP+ application on a system.

**Example**
The following command displays information about BSSAP+ in a Gs service named *gssvc1*.

```
show bssap+ statistics gs-service gssvc1
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show bssap+ statistics
show bulkstats

Displays the information on bulk statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show bulkstats [ [ data ] | [ schemas ] | [ variables [ apn | asngw | asnpc | bcmcs | card | closedrp | common | context | csfc | ecs | egtpc | fa | gprs | gtpc | gtpp | ha | ippool | ipsg | lac | lma | mag | mipv6ha | nat-realm | mme | pdif | pgw | phsgw | phspc | port | ppp | radius | rp | sccp | sgsn | sgtp | sgw | ss7link | ss7rd | system | vpn ] | obsolete ] ] [ | { grep grep_options | more }
```

data
Displays collected bulk statistical data.

schema
Displays the configuration of the statistics to be collected on a per-schema basis.

```
[ variables [ apn | asngw | asnpc | bcmcs | card | closedrp | common | context | csfc | ecs | egtpc | fa | gprs | gtpc | gtpp | ha | ippool | ipsg | lac | lma | mag | mipv6ha | nat-realm | mme | pdif | pgw | phsgw | phspc | port | ppp | radius | rp | sccp | sgsn | sgtp | sgw | ss7link | ss7rd | system | vpn ] | obsolete ]
```
Displays all valid bulkstat schema statistics, or only the statistics for the specified schema.
If the obsolete keyword is used, obsolete (but still available) schema variables are displayed. An asterisk (*) is displayed next to schema variables that have been obsoleted.
For information on available schemas, refer to the Bulk Statistics Configuration Mode Commands chapter.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For information on usage of grep and more, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
This command is used to display information on bulk statistics supported by the system.
The variable keyword can be used to list statistics supported by the system either for all schemas, or for an individual schema.
The schema keyword can be used to display the configuration of bulkstatistic settings including the schema.
The data keyword can be used to display bulkstatistic data collected up to that point.
Example
The following command displays the bulk statistics data:

```
show bulkstats data
```

The following command displays the bulk statistics schema configuration:

```
show bulkstats data schemas
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show card

Displays card information based upon the filtering options specified.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show card [ diag [ card_num ] | hardware [ card_num ] | info [ card_num ] | mappings | table [ all ] ] [ | { grep grep_options | more } ]
```

diag [ card_num ] | hardware [ card_num ] | info [ card_num ] | mappings | table [ all ]

Specifies what card information is to be displayed.

- `diag [ card_num ]`: indicates diagnostic information is to be displayed for all cards or the card specified by `card_num`. `card_num` must be a value in the range 1 through 48.
- `hardware [ card_num ]`: indicates information on the installed hardware is to be displayed for all cards or the card specified by `card_num`. `card_num` must be a value in the range 1 through 48.
- `info [ card_num ]`: indicates detailed information is to be displayed for all cards or the card specified by `card_num`. `card_num` must be a value in the range 1 to 48.
- `mappings`: indicates the front installed to rear installed card mapping is to be displayed.
- `table [ all ]`: indicates information for each card in front and RCC slots is to be displayed. The `all` keyword indicates all 48 slots are to be displayed.

```
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

View the card information to verify card installations for front and rear as well as for checking basic or detailed card information.

Example

The following command displays the diagnostic information for a card in slot 8:

```
show card diag 8
```

The following command displays the detailed information for a card in slot 8:

```
show card info 8
```

The following command displays the card mappings for the chassis:
show card mappings

The following command displays the card table:

show card mappings

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show cli

Displays current CLI users and associated session information.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show cli {session | history} [ | { grep grep_options | more } ]

- **session**
  Displays information about the current CLI session.

- **history**
  Displays CLI command history for this CLI session.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage
Show current command line interface sessions when there is some unexpected output from a chassis and a check of current CLI users may reveal other activities in progress.

Example
show cli
show clock

Displays the current system data and time.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show clock [ universal ] [ | { grep grep_options | more } ]
```

- **universal**
  Displays the date and time in universal coordinated time (UTC).

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Check the current time of a chassis to compare with network wide time or for logging purposes if network accounting and/or event records appear to have inconsistent timestamps.

**Important:** This command is not supported on all platforms.

Example
The following displays the system time in local time and UTC, respectively.

```
show clock
show clock universal
```
show configuration

Displays current configuration information for the card, context, port, or target configuration file as specified.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

show configuration [ card card_num | context name [ radius group [ all | name group]] | port slot/port | srp | [ showsecrets ] | [ url url | [ verbose ] ] { grep grep_options | more }]

card card_num | context name [radius group [all|name group]] | port slot/port

Specifies the type of configuration information to be displayed.

card card_num specifies a specific card for which configuration information is to be displayed.

card_num must be a value in the range 1 through 48.

context name specifies a specific context for which configuration information is to be displayed.

radius group[all|name group]: specifies a specific or all RADIUS server group/s configured in a specific context for which configuration information is to be displayed.

port slot/port: specifies a specific port for which configuration information is to be displayed.

srp

Shows the Service Redundancy Protocol configuration.

showsecrets

Show encrypted/unencrypted secret keys saved in the configuration. If this keyword is not specified, secret keys are not displayed.

url url

Default: configuration which is currently in use.

This keyword is not available to users with Operator level permissions. Specifies the location of the configuration data to use for information display. The url may refer to a local or a remote file. url must be entered using one of the following formats:

- ASR 5000:

  * [file:][/flash][/pcmcia1][/hd][/directory]/file_name
  * tftp://[host[:port]]/[directory]/file_name
  * [ http: | ftp: | sftp: ]//[/username[ :password]@]{host}[:port][/directory]/file_name

directory is the directory name.

filename is the actual file of interest.
**show configuration**

**Important:** Configuration files should be named with a .cfg extension.

- `username` is the user to be authenticated.
- `password` is the password to use for authentication.
- `host` is the IP address or host name of the server.
- `port#` is the logical port number that the communication protocol is to use.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

View the current configuration to review recent changes.

**Important:** This command is not supported on all platforms.

**Example**

The following command displays the local in use port configuration information for port 24/1 in verbose mode.

```
show configuration port 24/1 verbose
```

The following command displays the card configuration for card 17 on host `remoteABC` stored in the configuration file in `/pub/config.cfg`.

```
show configuration card 17
```

The following command displays the configuration of all RADIUS server groups configured in context `local`

```
show configuration context local radius group all
```

The following command shows the configuration for a context named PDIF.

```
show configuration context pdif
```
show configuration errors

Displays current configuration errors and warning information for the target configuration file as specified for a service.

Product
All

Privilege
Security Administrator, Administrator, Operator

Syntax

```
show configuration errors [ section { aaa-config | active-charging | apn |
asngw-service | asnpc-service | closed-rp-service | csclf-service | diameter |
fa-service | ggsn-service | gprs-service | gs-service | ha-service | hsgw-service |
imsh-service | imsue-service | ipms | ipsg-service | iups-service | lac-
service | lns-service | map-service | mme-service | pdif-service | pdns-service |
phsgw-service | policy-grp-config | sccp-network | sgsn-op-policy | sgsn-service |
sgtp-service | subscriber-config } } [ verbose ] [ | ( grep grep_options |
more ) ]
```

Specifies the services and section to display and validate configuration.

`aaa-config`: Displays configuration errors/warnings for the AAA service(s) configured on the system.

`active-charging`: Displays configuration errors/warnings for the Enhanced Charging Service(s) and the Personal Stateful Firewall service(s) configured on the system.

`apn`: Displays configuration errors/warnings for the APN configuration(s) on the system.

`asngw-service`: Displays configuration errors/warnings for the Access Service Network Gateway (ASN-GW) Service configured in a specific context for which configuration errors/warnings is to be displayed.

`asnpc-service`: Displays configuration errors/warnings for the Access Service Network Controller and Location Registry (ASN PC-LR) Service(s) configured on the system.

`closed-rp-service`: Displays configuration errors/warnings for the closed RP service(s) configured on the system.

`csclf-service`: Displays configuration errors/warnings for the Call Session Control Function (CSCF) service(s) configured on the system.

`diameter`: Displays configuration errors/warnings for the Diameter configuration(s) on the system.

`fa-service`: Displays configuration errors/warnings for the Foreign Agent (FA) service(s) configured on the system.

`ggsn-service`: Displays configuration errors/warnings for the GGSN service(s) configured on the system.

`gprs-service`: Displays configuration errors/warnings for the GPRS service(s) configured on the system.

`gs-service`: Displays configuration errors/warnings for the GS service(s) configured on the system.

`ha-service`: Displays configuration errors/warnings for the Home Agent (HA) service(s) configured on the system.

`hsgw-service`: Displays configuration errors/warnings for the HSGW service(s) configured on the system.
**imssh-service**: Displays configuration errors/warnings for the IMS Sh (IMSSh) service(s) configured on the system.

**imsue-service**: Displays configuration errors/warnings for the IMS UE service(s) configured on the system.

**ipms**: Displays configuration errors/warnings for the IPMS service(s) configured on the system.

**ipsg-service**: Displays configuration errors/warnings for the IP Security Gateway (IPSG) service(s) configured on the system.

**iups-service**: Displays configuration errors/warnings for the IuPS service(s) configured on the system.

**lac-service**: Displays configuration errors/warnings for the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) service(s) configured on the system.

**lns-service**: Displays configuration errors/warnings for the L2TP Network Server (LNS) service(s) configured on the system.

**map-service**: Displays configuration errors/warnings for the MAP service(s) configured on the system.

**mme-service**: Specifies the configuration errors for MME service configured in a specific context for which configuration errors/warnings is to be displayed.

**pdif-service**: Displays configuration errors/warnings for the PDIF service(s) configured on the system.

**pdsn-service**: Displays configuration errors/warnings for the PDSN service(s) configured on the system.

**phsgw-service**: Displays configuration errors/warnings for the PHS Gateway service(s) configured on the system.

**policy-grp-config**: Displays configuration errors/warnings for the Policy Group configuration(s) on the system.

**sccp-network**: Displays configuration errors/warnings for the SCCP network configuration(s) on the system.

**sgsn-op-policy**: Displays configuration errors/warnings for the SGSN operator policy configuration(s) on the system.

**sgsn-service**: Displays configuration errors/warnings for the SGSN service(s) configured on the system.

**sgtp-service**: Displays configuration errors/warnings for the SGTP service(s) configured on the system.

**subscriber-config**: Displays configuration errors/warnings for the subscriber configuration(s) on the system.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For more information on the usage of **grep** and **more**, refer *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view the current configuration errors and warning to review recent changes.

**Example**

The following command displays configuration errors and warnings for all services configured in a context/system:

```
show configuration errors verbose | more
```
The following command displays configuration errors and warnings for Enhanced Charging service and Personal Stateful Firewall service configured in a context:

```bash
d show configuration errors section active-charging verbose
```
show congestion-control

Displays information pertaining to congestion control functionality on the system

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show congestion-control { configuration | statistics { allmgr | asngwmgmgr | asnpcmgr | egtpinmgr | gtpcmgr | hamgr | l2tpmgr } [ all | instance task_instance ] } [ | { grep grep_options | more } ]

configuration

Displays congestion control configuration information including threshold parameters and policy settings for the configured services.

statistics

Displays congestion control statistics for one of the following services:

- allmgr: Specifies that statistics are displayed for PDSN services.
- asngwmgmgr: Specifies that statistics are displayed for ASN GW services.
- asnpcmgr: Specifies that statistics are displayed for ASN PC-LR services.
- egtpinmgr: Specifies that statistics are displayed for EGTP ingress demuxmgr.
- gtpcmgr: Specifies that statistics are displayed for GGSN services.
- hamgr: Specifies that statistics are displayed for HA services.
- l2tpmgr: Specifies that statistics are displayed for L2TP managers.
- all: Select this keyword to display statistics based on the current state of all instances of the specified task.
- instance task_instance: Specifies that statistics are to be displayed for a specific software task instance. task_instance can be configured to any integer value from 1 to 128.

Important: The inst column of the show task table command output can be used to determine the instance of a particular task.

grep grep_options | more

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

This command displays congestion control configuration information or statistics for a particular service type. When the all keyword is used, the system compares the current state of all instances of the specified task. The state is based on whether or not any congestion control thresholds have been exceeded. If one or more
instances are experiencing congestion, the state is displayed as “Applied”, and the various thresholds that have been crossed are indicated.

Example
The following command displays congestion control statistics for a PDSN service using an `allmgr` task with an instance of 2:

```
show congestion-control statistics allmgr instance 2
```

The following command displays congestion control statistics for an ASN GW service using an `asngwmgr` task with an instance of 2:

```
show congestion-control statistics asngwmgr instance 2
```

The following command displays congestion control statistics for an ASN PC-LR service using an `asnpcmgr` task with an instance of 2:

```
show congestion-control statistics asnpcmgr instance 2
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show content-filtering category database

This command displays details of the specified category based content filtering database for content filtering application configured in a system/service.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show content-filtering category database [ active | all | facility srdbmgr { all | instance instance_value } | url url_string] [ verbose ] [ | ( grep grep_options | more ) ]

active
Displays the information about all active databases, for example databases in memory. This is the default setting for category database information.

all
Displays the information about all active databases, for example, databases in memory and all saved databases on a system.

facility
Displays logged events for a specific facility.

srdbmgr { all | instance instance_value }
Displays logged events for all static rating database managers or for all or for a specific instance.

• all: Displays the logged events for all SRDB Manager instances.

• instance instance_value: Displays events logged for a specific SRDB Manager instance.

instance_value must be an integer from 1 through 8.

url url_string
Displays the information of the specific database located at the given URL. url_string specifies the name/location of category database to retrieve information, and must be an alpha and/or numeric string of 1 through 512 characters in length.

verbose
This option enables the detailed mode for additional information display for specific database.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
show content-filtering category database

Usage
Use this command to display information of database for category based content filtering application in a service.

Example
The following command displays a detailed information for all active databases in memory.

```
show content-filtering category database active all
```

The following command displays the CF database status of all running SRDB manager.

```
show content-filtering category database facility srdbmgr all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show content-filtering category policy-id

This command displays Content Filtering category policy definitions.

**Important:** In StarOS 8.1 and later this command is replaced by the `show active-charging content-filtering category policy-id` command.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```plaintext
show content-filtering category policy-id { all | id cf_policy_id } [ | { grep grep_options | more } ]
```

- **all**
  Displays definitions of all Content Filtering category policies.

- **id cf_policy_id**
  Displays definitions of a specific Content Filtering category policy.
  *cf_policy_id* must be a preconfigured category policy ID, and must be an integer from 1 through 4294967295.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view Content-Filtering Category definitions for a specific/all Policy IDs.

**Example**

The following command displays Content Filtering category definitions for policy ID 3:

```plaintext
show content-filtering category policy-id id 3
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show content-filtering category statistics

This command displays statistics for the Category-based Content Filtering application configured in a system/service.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show content-filtering category statistics [ facility srdbmgr { all | instance instance_value } volume { all | number } [ | { grep grep_options | more } ]

facility
Displays logged events for a specific facility.

srdbmgr { all | instance instance_value }
Displays logged events for all Static Rating Database Manager instances or for specified instance.
  • all: Displays events logged for all SRDB Manager instances.
  • instance instance_value: Displays events logged for a specific SRDB Manager instance.
    instance_value must be an integer from 1 through 8.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view the statistics of Category Based Content Filtering application in a service. This command’s output also indicates capability of the system to perform Content Filtering and Dynamic Content Filtering if configured.

Important: Content filtering cannot be performed if less than two PSCs are activated. Dynamic Content Filtering cannot be performed if less than three PSCs are activated.

Example
The following command displays the detailed statistics of configured category based content filtering application:

show content-filtering category statistics

The following command displays the detailed statistics of configured category based content filtering application based on running SRDB Manager instance1.
show content-filtering category statistics facility srdbmgr instance instance1

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show content-filtering category url

This command displays the information about the categories of the database at the specific URL configured for category based content filtering application in a system/service.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show content-filtering category url url_string [ policy-id cf_policy_id ] rulebase rulebase_name [ verbose ] [ | { grep grep_options | more } ]
```

**url url_string**
Displays the category information of the specific URL.
url_string specifies the URL, and must be an alpha and/or numeric string of 1 through 512 characters in length.

**policy-id cf_policy_id**
This option displays the category information of specific URL configured with specific content filtering category policy identifier in active charging configuration mode for category based content filtering. cf_policy_id must be a preconfigured category policy id in Active Charging Configuration Mode.

**rulebase rulebase_name**
This option displays the category information of specific URL configured in Active Charging Configuration mode for category based content filtering in specific Rulebase. rulebase_name must be the name of an existing rulebase, and must be an alpha and/or numeric string of 1 through 15 characters in length.

**verbose**
This option enables the detailed mode for additional information display for specific database.

**grep grep_options | more**
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to display information of a database URL for category based content filtering application in a service.

Example
The following command displays a detailed information for all active databases in memory.

```
show content-filtering category url verbose /cf_server/cf/optcmd.bin
verbose
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show content-filtering server-group

This command displays information for content Filtering Server Group (CFSG) configured in the service.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show content-filtering server-group [ name cfsg_name | statistics ] | [ | { grep grep_options | more } ]

name cfsg_name
Displays detailed information for the specified Content Filtering Server Group.

statistics
Displays statistical information for all configured Content Filtering Server Groups.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to display information for Content Filtering Server Group configured in a service.

Example
The following command displays a detailed information for all charging actions:

show content-filtering server-group statistics

The following command displays a details of a specific charging action:

show content-filtering server-group name sahre

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show context

Displays information on currently configured contexts.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show context [ all | name context_name ] [ | { grep grep_options | more } ]
```

```
all | name context_name
```

**all**: display information for all currently configured contexts.

**name context_name**: display information for the context specified as context_name only.

```
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

View configured contexts when the context of interest needs to be looked up. This may be useful in verifying configuration or in troubleshooting the system.

Example

The following command displays information for the configured context named *sampleContext*:

```
show context name sampleContext
```

The following command displays information for all contexts:

```
show context all
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show cpu

Displays information on system CPUs.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```bash
show cpu { info [ card card_num [ cpu cpu_num ] ] [ graphs ] [ verbose ] | table } [ grep grep_options | more ]
```

- **info [ card card_num [ cpu cpu_num ] ] [ graphs ] [ verbose ]**
  Specifies information for an entire card or a specific CPU is to be displayed.
  - `card` specifies the card to display associated information. `card_num` must be a value in the range 1 through 48 and must refer to an installed card.
  - `cpu` optionally selects a specific CPU on the card of interest to display specific information. `cpu_num` must be a value in the range 0 through 3 and must refer to an installed CPU.
  - `graphs`: in addition to textual CPU information display CPU utilization information in graphs.
  - `verbose`: output is to display all information available.

- **table**
  Display, in tabular format, all cards and CPUs.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

View CPU statistics to aid in diagnosing service problems for the case of overload conditions.

- **Important:** This command is not supported on all platforms.

Example

The following command displays the CPU information in tabular format for all CPUs on all installed cards:

```bash
show cpu table
```

The following command displays CPU information for card 8 in verbose mode:

```bash
show cpu info card 8 verbose
```
The following command displays information for CPU 0 on card 1:

```
show cpu info card 1 cpu 0
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
**show crash**

Displays summary of crashes or information on a specific crash.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show crash { list | number crash_num } [ | { grep grep_options | more } ]
```

**list | number crash_num**

*list:* indicates a list of recent crash data is to be displayed.

*number crash_num* indicates the information for the crash specified by `crash_num` is to be displayed. The crash number must be an existing crash which would be displayed using the `list` keyword.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

View the crash list to determine frequency of crashes or if crashes occur at some specific time of day. This may also be used to view information on a specific crash to aid in troubleshooting.

**Example**

The following displays the list of recent crashes.

```
show crash list
```

The following command will display the crash information for crash number 11.

```
show crash number 11
```
show credit-control sessions

This command displays credit control sessions information.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show credit-control session [ all | callid | full | mdn | nai | summary ] [ | { grep grep_options | more } ]

session [ all | callid | full | mdn | nai | summary ]
Displays the credit control session status based on the following keywords:
all: Displays all available information for Credit Control sessions
callid: Displays the Credit Control SessionCall ID
full: Displays all available information for the associated display or the filter keyword
mdn: Displays the Credit Control MDN
nai: Displays the Credit Control NI
summary: Displays the summary of Credit Control session information

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
Please refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference for details on the usage of grep and more.

Usage
Use this command to show active credit control application for service sessions.

Example
The following command shows the configured Credit control application sessions:

show credit-control sessions
show credit-control statistics

This command displays credit control statistics.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show credit-control statistics cc-service name
```

**cc-service**
Specifies the credit control service name.
*name* must be an existing Credit Control service, and must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**
Use this command to show active credit control statistics.

**Example**
The following command shows the configured credit control statistics for a service named *service1*:

```
show credit-control statistics cc-service service1
```
show crypto group

Displays information pertaining to configured crypto groups.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show crypto group [ name group_name| summary ]
```

- **name group_name**
  Displays information for a specific crypto group.
  - `group_name` is the name of the group for which to display information.

- **summary**
  Displays state and statistical information for configured crypto groups in this context.

Usage
Use this command to display information and statistics pertaining to one or all configured crypto groups within the current context.

If the `summary` keyword is not used, detailed information is displayed.

The following command displays detailed information for a crypto group called `group1`:

```
show crypto group name group1
```
show crypto ikev1

Displays pre-shared key information for peer security gateways configured within the context.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto ikev1 { keys | policy [preference] | security-associations [ summary ] }

keys
Specifies the IKE pre-shared key information based on the peer security gateway.

policy [ preference ]
Specifies the IKE policy priority for which configuration information will be displayed. The priority can be configured to any integer value from 1 to 100. If no preference is specified, information will be displayed for all configured policies.

security-associations [ summary ]
Specifies that established IPSec SA information should be displayed.

Usage
Use this command to:

- Display pre-shared key information. This information can be used to verify configuration and/or for troubleshooting.
- Verify the configuration of IKE policies within the context.
- Display established IPSec SA information. This information can be used for troubleshooting.

Example
The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto ikev1 keys
```

The following command displays information for an IKE policy with a preference of 1:

```
show crypto ikev1 policy 1
```

The following command displays the currently established SAs:

```
show crypto ikev1 security-associations summary
```
show crypto ikev2-ikesa security-associations summary

Summary view of ikev2-ikesa SAs

Product
PDIF

Privilege
Administrator, Security Administrator

Syntax

show crypto ikev2-ikesa security-associations summary

Usage
Shows a summary of the SAs configured for a crypto template. It shows the total configured SA lifetime in seconds and the number of seconds left on the timer.

Example
Use this command to create the SA summary:

    show crypto ikev2-ikesa security-associations summary

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show crypto ipsec

Displays IPSec security associations (SAs) configured within or facilitated by the context and can optionally display
statistics for them.

Product
PDSN, GGSN, PDIF, SCM

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show crypto ipsec security-associations map-type { ipsec-3gpp-cscf-subscriber | ipsec-dynamic | ipsec-ikev1 | ipsec-12tp | ipsec-manual | ipsec-mobile-ip } | summary [ distribution | ipsecmgr ipsec_mgr_id | map-type map_type ] | tag map_name
```

```
map-type { ipsec-dynamic | ipsec-ikev1 | ipsec-12tp | ipsec-manual | ipsec-mobile-ip }
```

Specifies that information for all crypto maps of a specific type configured within the context will be
displayed. The following types can be specified:
  • ipsec-3gpp-cscf-subscriber: P-CSCF Subscriber IPSec Tunnel
  • ipsec-dynamic: Dynamic IPSec Tunnel
  • ipsec-ikev1: IKEv1 IPSec Tunnel
  • ipsec-ikev2-subscriber: IKEv2 Subscriber Tunnel
  • ipsec-12tp: L2TP IPSec Tunnel
  • ipsec-manual: Manual (Static) IPSec Tunnel
  • ipsec-mobile-ip: Mobile IP IPSec Tunnel

```
summary [ distribution | ipsecmgr ipsec_mgr_id | map-type map_type | template-map map_name ]
```

Specifies that only security association summary information should be displayed.

distribution - Show IPSec Manager SA distribution information.
ipsecmgr ipsec_mgr_id - Show summary SA information for the specified IPSec manager instance ID.
  must be an integer from 1 through 200.
map-type map_type - Show summary SA information for the specified type of crypto map. The following
types can be specified:
  • ipsec-3gpp-cscf-subscriber: P-CSCF Subscriber IPSec Tunnel
  • ipsec-dynamic: Dynamic IPSec Tunnel
  • ipsec-ikev1: IKEv1 IPSec Tunnel
  • ipsec-12tp: L2TP IPSec Tunnel
  • ipsec-manual: Manual (Static) IPSec Tunnel
  • ipsec-mobile-ip: Mobile IP IPSec Tunnel
tag map_name

Specifies that SAs should be displayed for the specified crypto map.

*map_name* is the name of the crypto map configured in the context and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

### Usage

Use this command to display IPSec SA information and statistics. This information can be used for performance monitoring and/or troubleshooting.

The displayed information categorizes control signal and data statistics. Data statistics are further categorized according to the encapsulation method, either GRE or IP-in-IP.

### Example

The following command displays summary SA statistics for all IPSec managers.

```
show crypto ipsec security-associations summary
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show crypto ipsec transform-set

Displays IPsec transform set configuration information.

Product
PDG/TTG
PDIF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show crypto ipsec transform-set [ transform_name ]

transform_name
Specifies the name of a particular IPsec transform set for which to display information.
transform_name is the name of the IPsec transform set and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Usage
Use this command to verify the configuration of IPsec transform sets within the context.
If no keyword is specified, information will be displayed for all IPsec transform sets configured within the context.

Important: This command is used in PDIF Release 8.3 only.

Example
The following command displays information for an IPsec transform set named test1:

show crypto ipsec transform-set test1
show crypto isakmp keys

Displays pre-shared key information for peer security gateways configured within the context.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto isakmp keys

Usage
Use this command to display pre-shared key information based on the peer security gateway. This information can be used to verify configuration and/or for troubleshooting.

Example
The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

show crypto isakmp keys

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
**show crypto isakmp policy**

Displays ISAKMP policy configuration information.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show crypto isakmp policy [ preference ]
```

*preference*

Specifies the ISAKMP policy priority for which configuration information will be displayed. The priority can be configured to any integer value from 1 to 100.

**Usage**

Use this command to verify the configuration of ISAKMP policies within the context. If no *preference* is specified, information will be displayed for all configured policies.

**Example**

The following command displays information for an ISAKMP policy with a preference of 1:

```
show crypto isakmp policy 1
```
show crypto isakmp security-associations

Displays currently established IKE security associations (SAs) facilitated by the context.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show crypto isakmp security-associations [ cookies ]

cookies
Specifies that cookies should be displayed.
```

**Usage**

Use this command to display established IPSec SA information. This information can be used for troubleshooting.

**Example**
The following command displays the currently established SAs:

```
show crypto isakmp security-associations
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show crypto managers

Shows statistics per IPSec Manager.

Product
PDSN, GGSN, PDIF, SCM

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto managers [ context context_id | crypto-map map_name | instance instance_num | summary [ distribution | ike-stats | ipsec-3gpp-cscf-stats | ikev2-stats [ demux-stats ] | ipsec-sa-stats | npu-stats ] ]

context context_id
Show IPSec manager statistics for the context with the specified context identifier number. must be an integer from 1 through 64.

crypto-map map_name
Show IPSec Managers for a specific crypto map. map_name must be the name of an existing crypto map.

instance instance_num
Show statistics for the specified IPSec manager instance. instance_num must be an integer from 1 through 284.

summary [ distribution | ike-stats | ipsec-3gpp-cscf-stats | ikev2-stats [ demux-stats ] | ipsec-sa-stats | npu-stats ]
Shows stats per service ip address for each manager.

distribution - Shows a summary list of IPsec manager distribution.
ike-stats - Shows a summary list of IPsec IKE statistics for each IPsec manager.
ipsec-3gpp-cscf-stats - Displays CSCF IPSec Statistics on each IPsec Manager.
ikev2-stats - Displays IKEv2 Statistics on each IPsec Manager.
*demux-stats - Displays session demux statistics on each IPsec Manager.
ipsec-sa-stats - Shows a summary list of IPsec Security Association statistics for each IPsec Manager.
npu-stats - Displays NPU statistics on each IPsec Manager.

Usage
Use this command to view statistics relating to IPSec managers.

Example
The following command displays summary information for all IPsec managers:

show crypto managers summary
Important: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show crypto map

Displays crypto map configuration information.

Product
PDIF, PDSN, GGSN, SCM

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
```
show crypto map [ map-type [ ipsec-3gpp-cscf-subscriber | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip ] |
tag map_name | summary ]
```

**map-type [ ipsec-3gpp-cscf-subscriber | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip ]**

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:
- **ipsec-3gpp-cscf-subscriber**: P-CSCF subscriber IPSec Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

**tag map_name**

Specifies the name of a crypto map for which to display configuration information. *map_name* is the name of the crypto map configured in the context and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

**summary**

Displays summary information for all crypto maps configured in the context.

Usage

Use this command to verify the configuration of crypto maps within the context.
If no keyword is specified, information will be displayed for all maps configured within the context regardless of type.

Example

The following command displays configuration information for a dynamic crypto map named *test_map3*:

```
show crypto map tag test_map3
```
Exec Mode Show Commands (A-C)

show crypto map
show crypto statistics

Displays IPSec statistics.

Product
PDSN, GGSN, PDG/TTG, PDIF, SCM

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show crypto statistics ikev1 | ikev2 [service-ip-address ip-address ] [ service-name name ] | ipsec-3gpp-cscf [ service-ip-address ip-address ] [ service-name name ]
```

---

**ikev1**
Displays global ikev1 statistics for this context.

```
ikev2 [ service-ip-address ip-address ] [ service-name name ]
```
Displays global ikev2 statistics for this context.

- **service-ip-address ip-address**: Specified PDIF service ip address.
- **service-name name**: Specified PDIF service name.

```
ipsec-3gpp-cscf [ service-ip-address ip-address ] [ service-name name ]
```
Displays global CSCF IPSec SA statistics for this context.

- **service-ip-address ip-address**: Specified CSCF service ip address.
- **service-name name**: Specified CSCF service name.

---

**Usage**
Use this command to display statistics for IPSec tunnels facilitated by the context. This information can be used for performance monitoring and/or troubleshooting.

---

**Example**
The following command displays cumulative IPSec statistics for the current context:

```
show crypto statistics
```

---

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show crypto transform-set

Displays transform set configuration information.

**Product**
PDIF, PDSN, GGSN, SCM

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show crypto transform-set [ transform_name ]
```

*transform_name*

Specifies the name of a particular transform set for which to display information. *transform_name* is the name of the transform set and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

**Usage**
Use this command to verify the configuration of transform sets within the context. If no keyword is specified, information will be displayed for all transform sets configured within the context.

**Important:** This command is used in PDIF Release 8.1. In PDIF Release 8.3, the syntax of this command is changed to `show crypto ipsec transform-set`.

**Example**
The following command displays information for a transform set named test1:

```
show crypto transform-set test1
```
show cscf nat

Displays the mapping created for each of the media streams present in an established dialog.

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator

Syntax

```
show cscf nat media mapping { all | aor aor } [ | { grep grep_options | more } ]
```

**media mapping { all | aor aor }**

*all*: Displays the UE/Network origins and destinations, including their IP addresses/port numbers and associated contexts.

*aor aor*: Displays information for a specific AoR. *aor* must be an existing AoR and be from 1 to 79 alpha and/or numeric characters.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference for details on the usage of `grep` and `more`.

Usage

Use this command to display the status of configured Network Address Translation (NAT) support.

Example

The following command displays the status of the mapping created for each of the media streams present on this system:

```
show cscf nat media mapping all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf peer-servers

Displays name, IP address, and status of configured peer servers visible to the system.

**Product**
SCM

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
show cscf peer-servers { all | full | name service_name [ server-name server_name ] } [ | { grep grep_options | more } ]
```

- **all | full**: Displays the peer server list names and the servers within those lists including their IP addresses/port numbers and domain names.
- **name service_name [ server-name server_name ]**: Displays the same information as the full keyword output, but for a specific peer server list or specific server.
- **service_name/server_name**: Must be an existing peer server list or server and be from 1 through 80 alpha and/or numeric characters.
- **grep grep_options | more**: Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference for details on the usage of `grep` and `more`.

**Usage**

Use this command to display the status of configured peer servers.

**Example**

The following command displays the status of a peer server named `icscf3` that is a member of peer server list `cscf-main`:

```
show cscf peer-servers name cscf-main server-name icscf3
```

The following command displays the status of all peer servers in configured peer server groups in this context:

```
show cscf peer-servers full
```

**Important**: Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf service

Displays configuration and/or statistic information for CSCF services on this system.

**Product**

SCM

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
show cscf service { all [ counters ] | diameter [ location-info statistics service-name service_name [ vpn-name name ] | policy-control statistics service-name service_name [ vpn-name name ] ] | grey-list name name | li-packet-cable statistics service-name service_name | performance-counters name service_name | statistics name service_name [ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp ] | subscription name service_name } [ | ( grep grep_options | more ) ]
```

**all [ counters ]**

Displays configuration information for all CSCF services configured on this system.

**counters:** Displays statistics with the configuration information for all CSCF services configured on the system.

**diameter [ location-info statistics service-name service_name [ vpn-name name ] | policy-control statistics service-name service_name [ vpn-name name ] ]**

**location-info:** Displays Diameter statistics on the E2 interface with the location information.

**policy-control:** Displays Diameter (DPECA) statistics on the CSCF Rx interface with the configuration information.

**service-name service_name:** Specifies the name of a CSCF service for which the statistics will be displayed. *service_name* must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

**vpn-name name:** Specifies the name of a context in which all statistics for all services will be displayed. *name* must be an existing context and be from 1 to 79 alpha and/or numeric characters.

**grey-list name name**

Displays the list of run-time grey-listed users and their remaining barred period for the specified CSCF service.

**name** must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

**li-packet-cable statistics service-name service_name**

Displays Lawful Intercept statistics for a specific CSCF service configured on this system. *service_name* must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.
performance-counters name service_name
Displays performance counters specified in 3GPP TS 32.409 for a specific CSCF service configured on this system. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

statistics name service_name [ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp | vpn-name name ]
Displays service statistics for a specific CSCF service configured on this system. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.
all: Displays all CSCF service statistics.
calls: Displays session statistics related to CSCF calls.
ip-security: Displays session statistics related to CSCF IPsec.
message: Displays session statistics for the SIP method MESSAGE.
package-name: Displays session statistics for the associated event package.
  • message-summary: Displays session statistics for the “message-summary” event package.
  • presence: Displays session statistics for the “presence” event package.
  • reg: Displays session statistics for the “reg” event package.
  • winfo: Displays session statistics for the “watcher-info” event package.
registrations: Displays session statistics related to CSCF registrations, re-registrations, and de-registrations.
sigcomp: Displays session statistics related to CSCF sigcomp.
tcp: Displays session statistics related to CSCF TCP.

Important: This keyword must be followed by another statistics-related keyword.

subscription name service_name
Displays service level subscription information for a specific service. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to display configuration information and/or statistics for any or all CSCF services on this system.

Example
The following command displays service statistics for the CSCF service named cscf1:

  show cscf service statistics name cscf1
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show cscf sessions

Displays statistics for CSCF sessions on this system.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Syntax

show cscf sessions { counters { calls { duration | first-response-time | invite-processing-time | post-answer-delay | post-dial-delay | service service_name | session-release-delay | session-setup-delay } service service_name | subscription { duration | service service_name | setup-time } service service_name } | duration | full [ callleg-id id | from-aor aor | service service_name | session-id id | to-aor aor ] [ media-type type ] | summary [ from-aor aor | service service_name | session-id id | to-aor aor ] } [ | { grep grep_options | more } ]

counters { calls { duration | first-response-time | invite-processing-time | post-answer-delay | post-dial-delay | service service_name | session-release-delay | session-setup-delay } service service_name | subscription { duration | service service_name | setup-time } service service_name }

Important: This keyword may be used alone with the counters keyword or following any other counters-specific keyword.

• duration: Displays the call duration time.
• first-response-time: Displays the time interval for the first response received for INVITE.
• invite-processing-time: Displays the INVITE message processing time in CSCF.
• post-answer-delay: Displays the time interval for post answer delay.
• post-dial-delay: Displays the time interval for the ringing or success response for INVITE.
• service service_name: Displays specific service. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

Important: This keyword may be used alone with the counters keyword or following any other counters-specific keyword.

• session-release-delay: Displays the time interval for releasing the call.
• session-setup-delay: Displays the time interval for session setup.

subscription: Counters associated with subscriptions in CSCF service.
• duration: Displays the SIP Subscription duration time.
• service service_name: Displays specific service. service_name must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.
**show cscf sessions**

***Important:** This keyword may be used alone with the `subscription` keyword or following any other subscription-specific keyword.

- **setup-time:** Displays the SIP Subscription setup time.

**duration**

Displays the call duration for all CSCF sessions.

```
full [callleg-id id | from-aor aor | service service_name | session-id id | to-aor aor] [ media-type type ]
```

Displays all the session information for the active CSCF sessions matching the filter criteria.

- **callleg-id id:** Specifies a call leg from which session statistics are to be displayed. `id` must be an existing call-leg ID and be from 1 to 63 alpha and/or numeric characters.
- **from-aor aor:** Specifies that session statistics are to be displayed for sessions originating from this specific AoR. `aor` must be an existing AoR and be from 1 to 79 alpha and/or numeric characters.
- **service service_name:** Specifies that session statistics are to be displayed for sessions using this CSCF service. `service_name` must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.
- **session-id id:** Specifies that session statistics are to be displayed for sessions with this ID. `id` must be an existing session ID and be from 1 to 63 alpha and/or numeric characters.
- **to-aor aor:** Specifies that session statistics are to be displayed for sessions sent to this specific AoR. `aor` must be an existing AoR and be from 1 to 79 alpha and/or numeric characters.
- **media-type type:** Displays information about specific media type, if any. `type` must be an existing media type and be from 1 to 9 alpha and/or numeric characters.

```
summary [ from-aor aor | service service_name | session-id id | to-aor aor ]
```

Displays session summary information for sessions matching the filter criteria.

- **from-aor aor:** Specifies that session statistics are to be displayed for sessions originating from this specific AoR. `aor` must be an existing AoR and be from 1 to 79 alpha and/or numeric characters.
- **service service_name:** Specifies that session statistics are to be displayed for sessions using this CSCF service. `service_name` must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.
- **session-id id:** Specifies that session statistics are to be displayed for sessions with this ID. `id` must be an existing session ID and be from 1 to 63 alpha and/or numeric characters.
- **to-aor aor:** Specifies that session statistics are to be displayed for sessions sent to this specific AoR. `aor` must be an existing AoR and be from 1 to 79 alpha and/or numeric characters.

```
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

Refer to **Regulating a Command’s Output** section of the **Command Line Interface Overview** chapter in the **Command Line Interface Reference** for details on the usage of `grep` and `more`.

**Usage**

Use this command to display session information for any or all CSCF sessions.
Example
The following command displays the output for CSCF session duration:

```
show cscf sessions duration
```

⚠️ **Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
**show cscf sip**

Displays SIP statistics for a specific CSCF service configured on this system.

**Product**

SCM

**Privilege**

Security Administrator, Administrator, Operator

**Syntax**

```
show cscf sip statistics name service_name [ interface { domain { list | name domain_name } | ip { address ip_address | list } } | vpn-name name ] [ | { grep grep_options | more } ]
```

**show cscf sip statistics name service_name**

Specifies the name of the CSCF service. `service_name` must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

```
[ interface { domain { list | name domain_name } | ip { address ip_address | list } }
```

SIP statistics will be displayed for this interface.

**domain list:** Displays list of interfaces associated with the CSCF service.

**domain name domain_name:** Specifies the domain associated with the CSCF service. `domain_name` must be an existing domain and be from 1 to 64 alpha and/or numeric characters.

**ip address ip_address:** Specifies the destination or source ip address associated with the CSCF service.

**ip list:** Displays list of interfaces associated with the CSCF service.

**vpn-name name**

Specifies the name of the context in which the service is configured. `name` must be an existing context and be from 1 to 79 alpha and/or numeric characters.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. Refer to *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference* for details on the usage of `grep` and `more`.

**Usage**

Use this command to display SIP statistics for a specific CSCF service.

**Important:** This command displays counters for SIP statistics for a specified CSCF service. Counters are incriminated when SIP messages are sent (Tx) or received (Rx). SIP Request, Response, and Error counters are maintained at various levels in the SIP stack. These values are dependent on the packet flow. For example, if packets are dropped at an initial stage of parsing and error detection, the counters may not increment. All 2xx Response counters for
individual requests are maintain outside the SIP layer and will not track re-transmissions and erroneous packets that are dropped. All other counters do keep track of re-transmissions.

Example
The following command displays SIP statistics for the CSCF service named cscf1:

```
show cscf sip statistics name cscf1
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf tcp

Displays TCP connection information for a specific CSCF service configured on this system.

**Product**
SCM

**Privilege**
Security Administrator, Administrator, Operator

**Syntax**

```
show cscf tcp connections service service_name [ facility { cscfmg | sessmgr } ] [ full ] [ remote-ip ip_address ] [ remote-port port_number ] [ | { grep grep_options | more } ]
```

- **connections service service_name**
  - Specifies the name of the CSCF service.
  - Must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

- **facility { cscfmg | sessmgr }**
  - Facility type for which connection details have to be retrieved.
  - **cscfg**: Facility type cscfmg.
  - **sessmgr**: Facility type sessmgr.

- **full**
  - Displays detailed information related to each connection.

- **remote-ip ip_address**
  -Remote IP address to match the connection. `ip_address` is expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **remote-port port_number**
  - Remote port to match the connection.

- **grep grep_options | more**
  - Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - Refer to **Regulating a Command’s Output** section of the **Command Line Interface Overview** chapter in the **Command Line Interface Reference** for details on the usage of **grep** and **more**.

**Usage**

Use this command to display TCP connection information for a specific CSCF service.

**Important:** More than one optional keyword may be used per command.
Example
The following command displays TCP connections for the CSCF service named *cscf1*:

```
show cscf tcp connections service cscf1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show css delivery-sequence

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.
show css server

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.
show css service

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.
Chapter 93
Exec Mode Show Commands (D-G)

This section includes the commands `show dhcp` through `show gtpu-service`.
show dhcp

Displays counter information pertaining to DHCP functionality based on specific criteria.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show dhcp [ counters | full | summary ] [ all | apn apn_name | callid id | chaddr mac_address | dhcp-service svc_name | imsi imsi | user-address address | msid msid | server server_address | username name ]
```

counters
Displays DHCP counter information.

full
Displays all available information pertaining to the criteria specified.

summary
Displays a summary of the DHCP statistics.

all
Displays counter information for each active PDP context.

apn apn_name
Displays information based on a specific APN name.
apn_name is the name of the APN and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

callid id
Displays information for a specific call identification number.
id must be specified as a 4-byte hexadecimal number.

chaddr mac_address
Displays information for a specific mobile node.
mac_address must be MAC address of mobile node.

dhcp-service svc_name
Displays information for a specific DHCP service.
svc_name is the name of the DHCP service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.
**imsi imsi**
Displays information for a specific International Mobile Subscriber Identity (IMSI).
*imsi* is an integer value from 1 to 15 characters.

**user-address address**
Displays information for a specific DHCP-assigned user IP address.
*address* is the IP address expressed in dotted-decimal notation.

**msid msid**
Displays information for a specific Mobile Subscriber Identity (MSID).
*msid* must be from 1 to 15 digits.

**server server_address**
Displays information for a specific DHCP server.
*server_address* is the IP address of the server expressed in dotted-decimal notation.

**username name**
Displays information for a specific subscriber.
*name* can be from 1 to 127 alpha and/or numeric characters (including wildcards (‘$’ and ‘*’)) and is case sensitive.

**Usage**
Counters pertaining to DHCP functionality can be displayed as cumulative values or for specific APNs, PDP contexts, servers, or DHCP services.

**Example**
The following command displays DHCP counter information for a DHCP service called DHCP-Gi:

```
show dhcp dhcp-service DHCP-Gi
```

The following command displays DHCP counter information for a DHCP Call Id 01ca11a2:

```
show dhcp call-id 01ca11a2
```

The following command displays DHCP information for the specified mobile node:

```
show dhcp chaddr 00:05:47:00:37:44
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show dhcp statistics

Displays DHCP statistics for the specified servers.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show dhcp statistics [ dhcp-service svc_name | server ip_address ]
```

- **dhcp-service svc_name**
  Displays statistics for a specific DHCP service.
  `svc_name` is the name of the desired DHCP service and can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.

- **server ip_address**
  Displays statistics for a specific DHCP server.
  `ip_address` is the IP address of the desired server and must be entered in dotted decimal notation.

Usage
Statistics for a single DHCP service or DHCP server can be viewed using the `dhcp-service` or `server` keywords respectively.
Cumulative statistics for all DHCP services and servers within a context can be viewed by executing the command with no keywords from within the context in which they’re configured.
If this command is issued from within the local context, the statistics displayed will be cumulative for all dhcp servers configured on the system regardless of context.

Example
The following command allows you to view statistics for all configured DHCP servers within the context:

```
show dhcp statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show dhcp-service

Displays configuration information for either a specific, or for all DHCP servers configured.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show dhcp-service { all | name svc_name }
```

- **all**
  Displays information for all configured DHCP services.

- **name svc_name**
  Displays information for a specific DHCP service.
  `svc_name` is the name of the service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Usage
This command is used to verify the configuration of one or all DHCP services for monitoring or troubleshooting purposes. The output is a concise listing of DHCP service parameter settings. If this command is executed from within the local context with the all keyword, information for all DHCP services configured on the system will be displayed.

Example
The following command displays configuration information for a DHCP service called dhcp1:

```
show dhcp-service name dhcp1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show dhcp status

Displays configuration information for either a specific, or for all DHCP service and servers configured.

Product
GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show dhcp status [ dhcp-service svc_name ] [ server ip_addr ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays information for all configured DHCP services.</td>
</tr>
<tr>
<td>dhcp-service svc_name</td>
<td>Displays information for a specific DHCP service. svc_name is the name of the service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.</td>
</tr>
<tr>
<td>server ip_address</td>
<td>Displays status for a specific DHCP server. ip_address is the IP address of the desired server and must be entered in dotted decimal notation.</td>
</tr>
</tbody>
</table>

Usage
This command is used to show/verify the status or configuration of one or all DHCP services along with count of cumulative leased addresses and addresses leased at that time for monitoring or troubleshooting purposes. The output is a concise listing of DHCP service parameter settings.
If this command is executed from within the local context with the all keyword, information for all DHCP services configured on the system will be displayed.

Example
The following command displays status of a DHCP service called ggsn_dhcp1:

```
show dhcp status dhcp-service ggsn_dhcp1
```

State shown in display is consolidated across session managers, i.e. for each session manager, DHCP server have a timestamp value associated with its state.
For a DHCP server, its timestamp value is compared for each session manager and the state associated with the latest value is shown.

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show diameter aaa-statistics

This command displays Diameter AAA statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show diameter aaa-statistics [ all | group group_name [ server server_name ] | server server_name ] [ | { grep grep_options | more } ]
```

- **all**
  Displays all available Diameter server statistics.

- **group group_name [ server server_name ]**
  Displays all Diameter server statistics within the specified AAA group.
  
  - *group_name* must be the name of a AAA group, and must be a string of 1 through 64 characters in length.
  
  - *server_name* must be the name of a Diameter server, and must be a string of 1 through 64 characters in length.

- **server server_name**
  Displays Diameter server statistics for the specified server.
  
  - *server_name* must be the name of the Diameter server, and must be a string of 1 through 64 characters in length.

  | { grep grep_options | more } |
  |
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output must be specified.

  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

Use this command to view Diameter AAA statistics.

**Example**

The following command displays all available Diameter server statistics:

```
show diameter aaa-statistics all
```
show diameter accounting servers aaa-group

This command displays Diameter accounting server information for a AAA group.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show diameter accounting servers [ aaa-group group_name ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>group_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_name must be the name of a AAA group, and must be a string of 0 through 64 characters in length.</td>
</tr>
</tbody>
</table>

|  | { grep grep_options | more } |
|-----------------|-------------------|
| Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified. |
| For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference. |

**Usage**

Use this command to view Diameter accounting server information for a AAA group.

**Example**
The following command displays Diameter accounting server information for a AAA group named `group12`:

```
show diameter accounting servers aaa-group group12
```
show diameter authentication servers aaa-group

This command displays Diameter Authentication server information for a specified AAA group.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show diameter authentication servers [ aaa-group group_name ]
```

*group_name*

*group_name* must be the name of a AAA group, and must be a string of 0 through 64 characters in length.

**Usage**

Use this command to view Diameter authentication server information for a AAA group.

**Example**
The following command displays Diameter authentication server information for a AAA group named *group12*:

```
show diameter authentication servers aaa-group group12
```
show diameter endpoint

This command has been deprecated, and is replaced by the `show diameter endpoints` command.
show diameter endpoints

This command displays the status of Diameter client endpoint(s).

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show diameter endpoints { all | endpoint endpoint_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays status of all Diameter client endpoints.

- **endpoint endpoint_name**
  Displays status of the specified Diameter client endpoint. 
  `endpoint_name` must be the name of a Diameter endpoint, and must be a string of 1 through 63 characters in length.

- **| { grep grep_options | more }**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view the status of Diameter client endpoints.
If you are in the local context, then all contexts are searched for the specified endpoint(s). Specify `all` to see all endpoints; otherwise, just the named endpoint will be displayed. If no argument is provided, a summary of all endpoints is displayed.
Default value: N/A

Example
The following command displays status of all Diameter client endpoints.

```
show diameter endpoints all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show diameter message-queue

This command displays Diameter message queue statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter message-queue counters { inbound | outbound } [ endpoint endpoint_name [ peer-host peer_id [ peer-realm realm_id ] ] | session-id session_id ] [ | { grep grep_options | more } ]

counters { inbound | outbound }
Specifies the message counters:
  inbound: Specifies Diameter inbound messages
  outbound: Specifies Diameter outbound messages

endpoint endpoint_name
Specifies the Diameter endpoint.
endpoint_name must be a string of 1 through 63 characters in length.

peer-host peer_id
Specifies the Diameter peer host.
peer_id must be a string of 1 through 63 characters in length.

peer-realm realm_id
Specifies the Diameter peer realm.
realm_id must be a string of 1 through 127 characters in length.

session-id session_id
Specifies the session ID.
session_id must be a string of 1 through 127 characters in length.

| { grep grep_options | more }
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view the count of the messages in the Diameter message queue for specific counter type, session ID, or endpoint, peer host, and peer realm.
Example
The following command displays message queue statistics for outbound messages specific to the Diameter endpoint named `asr5k.testnetwork.com`:

```
show diameter message-queue counters outbound endpoint asr5k.testnetwork.com
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show diameter peers

This command displays Diameter peer information.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter peers [ full | summary ] [ all | [ endpoint endpoint_name ] [ peer-host peer_id ] [ peer-realm realm_id ]+ ] [ | { grep grep_options | more } ]

| full
| Displays full details of all or specified Diameter peers.

| summary
| Displays summary details of all or specified Diameter peer(s).

| all
| Displays details of all Diameter peers.

| endpoint endpoint_name
| Displays details of the specified Diameter endpoint.
endpoint_name must be the origin endpoint value, and must be a string of 1 through 255 characters in length.

| peer-host peer_id
| Displays details of the specified Diameter peer host.
peer_id must be the peer host value, and must be a string of 1 through 63 characters in length.

| peer-realm realm_id
| Displays details of the specified Diameter peer realm.
realm_id must be the Diameter peer realm ID, and must be a string of 1 through 127 characters in length.

| | { grep grep_options | more }
| Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view the details of Diameter peers.
If you are in the local context, then all contexts are searched for the specified peer(s). This is similar to the `show subscribers` CLI command and supports multiple filter options specified at the same time.

If filter options are specified (e.g., `all,endpoint`, etc.), the default is for one line of output to be displayed per peer. Use `full` to get detailed information per peer, or `summary` to get summarized information about all matching peers.

If no filter options are specified, a summary output for all peers is displayed. Use the `full` option to get detailed information about every peer.

Default value: N/A

**Example**
The following command details of the Diameter endpoint named `endpoint12`:

```
show diameter peers endpoint endpoint12
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show diameter route status

This command displays Diameter route health status information.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show diameter route status [ endpoint endpoint_name | full [ endpoint endpoint_name ] ] [ host host_name | peer peer_id ] [ | { grep grep_options | more } ]
```

---

**full**
Displays information of which Diameter clients are using which peer/host combinations.

---

**endpoint endpoint_name**
Displays detailed information of the specified Diameter client endpoint.
*endpoint_name* must be the name of a Diameter endpoint, and must be a string of 1 through 63 characters in length.

---

**host host_name**
Displays information for the specified Diameter host.
*host_name* must be the name of a Diameter host, and must be a string of 1 through 63 characters in length.

---

**peer peer_id**
Displays information for the specified Diameter peer.
*peer_id* must be the name of a Diameter peer host, and must be a string of 1 through 63 characters in length.

---

```
| { grep grep_options | more }
```
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of *grep* and *more*, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

---

**Usage**
Use this command to view the Diameter route health status.
The route status displays status of peer/host combinations. Refer to the *route-failure* CLI command in Diameter Endpoint Configuration mode. When no options are specified, the display will give one line per peer/host combination, indicating how many Diameter clients are using each combination, and for how many clients the combination is available or failed. Specify *full* to see which Diameter clients are using which peer/host combinations. Specify *host* or *peer* to see just combinations with the named host or peer. Specify *endpoint* to see detailed information about the named Diameter client.
Default value: N/A

Example
The following command displays route health status details of the Diameter client endpoint named `endpoint12`:

```
show diameter route status endpoint endpoint12
```
show diameter route table

This command displays the Diameter routing table.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter route table [ wide ] [ endpoint endpoint_name ] [ | { grep grep_options | more } ]

wide
Displays the route table information in wide-format.

endpoint endpoint_name
Displays the Diameter routing table for the specified endpoint.

endpoint_name must be the name of a Diameter endpoint, and must be a string of 1 through 63 characters in length.

| { grep grep_options | more }

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view the status of Diameter client endpoints.
If you are in the local context, then the route information used by Diameter endpoints in all chassis contexts will be used in the display.
The route table displays all static and dynamic routes. Refer to the route-entry CLI command in Diameter Endpoint Configuration Mode.
Default value: N/A

Example
The following command displays status of the Diameter client endpoint named endpoint12.

    show diameter route table endpoint endpoint12
show diameter statistics

This command displays Diameter peer statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show diameter statistics [ [ proxy ] endpoint endpoint_name [ peer-host peer_id [ peer-realm realm_id ] ] ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>endpoint endpoint_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays statistics for the specified Diameter endpoint.</td>
</tr>
<tr>
<td><code>endpoint_name</code> must be the name of a Diameter endpoint, and must be an alpha and/or numeric string of 1 through 63 characters in length.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>peer-host peer_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays statistics for the specified Diameter host peer.</td>
</tr>
<tr>
<td><code>peer_id</code> must be an alpha and/or numeric string of 1 through 255 characters in length.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>peer-realm realm_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays statistics for the specified Diameter peer realm.</td>
</tr>
<tr>
<td><code>realm_id</code> must be an alpha and/or numeric string of 1 through 127 characters in length.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays proxy related statistics.</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more } |
|-------------------|
| Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified. |
| For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference. |

Usage

Use this command to view Diameter statistics for the specified endpoint or proxy.

Example

The following command displays Diameter peer statistics for the endpoint named `endpoint12`:

```
show diameter statistics endpoint endpoint12
```
show dns-client

Displays DNS cache and/or statistics for a specified DNS client.

Product
P-CSCF, SIP Proxy, SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show dns-client { cache client name [ query-name name | query-type { A | SRV } ] | statistics client name } [ | { grep grep_options | more } ]

**cache client name [ query-name name | query-type { A | SRV } ]**

Specifies that the cache for the defined DNS client is to be displayed.

**name**: Defines the name of the DNS client whose cache is to be displayed. **name** must be an existing DNS client and be from 1 to 255 alpha and/or numeric characters in length.

**query-name name**: Filters DNS results based on the domain name. **name** must be from 1 to 255 characters in length. **name** is the domain name used to perform the DNS query. **name** is different from the actual domain name which is resolved. For example, to resolve the SIP server for service.com, the query name is _sip._udp.service.com and the query type is SRV.

**query-type**: Filters DNS results based on domain IP address records (A records).

- **A**: Filters DNS results based on domain IP address records (A records).
- **SRV**: Filters DNS results based on service host records (SRV records).

**statistics client name**

Specifies that statistics for the defined DNS client are to be cleared.

**name**: Defines the name of the DNS client whose statistics are to be displayed. **name** must be an existing DNS client and be from 1 to 255 alpha and/or numeric characters in length.

| { grep grep_options | more } |

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 5000 Series Command Line Interface Reference.

Usage

Use this command to display DNS cache and/or statistics for a specified DNS client.

Example

The following command displays statistics for a DNS client named domain1.com

```
show dns-client statistics client domain1.com
```
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show dynamic-policy statistics

Displays policy control and charging (PCC) statistics from the interface communicating with the PCRF (Gx(x)).

**Product**

HSGW, PDSN, S-GW

**Privilege**

Inspector

**Syntax**

```
show dynamic-policy statistics { hsgw-service name | pdsn-service name | sgw-service name }
```

- **hsgw-service name**
  
  Displays policy control and charging statistics from the Gxa interface communicating with the PCRF. *name* must be an existing HSGW service name and be from 1 to 63 alpha and/or numeric characters.

- **pdsn-service name**
  
  Displays policy control and charging statistics from the Gx interface communicating with the PCRF. *name* must be an existing PDSN service name and be from 1 to 63 alpha and/or numeric characters.

- **sgw-service name**
  
  Displays policy control and charging statistics from the Gxc interface communicating with the PCRF. *name* must be an existing S-GW service name and be from 1 to 63 alpha and/or numeric characters.

**Usage**

Use this command to display PCC statistics for the specified service and its Gx interface communicating with the PCRF.

**Example**

The following command displays PCC statistics for a PDSN service named *cdma4*:

```
show dynamic-policy statistics pdsn-service cdma4
```
show egtpc peers

Displays information about eGTP-C peers.

Product
MME, P-GW, S-GW

Privilege
Inspector

Syntax

show egtpc peers [ address ip_address | egtp-service name [ address ip_address ] | interface { mme [ address ip_address ] | pgw-ingress [ address ip_address ] | sgw-egress [ address ip_address ] | sgw-ingress [ address ip_address ] } ] [ | { grep grep_options | more } ]

address ip_address

Displays information about a specific eGTP-C peer based on the IP address of the peer. ip_address must be an existing eGTP-C peer and be expressed in IPv4 dotted decimal notation.

egtp-service name [ address ip_address ]

Displays information about eGTP-C peers associated with a specific service. name must be an existing egtp-service and be from 1 to 63 alpha and/or numeric characters.

address ip_address: Additionally, the results can be filtered based on the IP address associated with the service. ip_address must be an existing eGTP-C peer and be expressed in IPv4 dotted decimal notation.

interface { mme [ address ip_address ] | pgw-ingress [ address ip_address ] | sgw-egress [ address ip_address ] | sgw-ingress [ address ip_address ] }

Displays information about eGTP-C peers associated with the service interface configured on this system.

mme [ address ip_address]: Displays information about eGTP-C MME peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the MME peer. ip_address must be an existing MME peer and be expressed in IPv4 dotted decimal notation.

pgw-ingress [ address ip_address ]: Displays information about eGTP-C P-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the P-GW ingress peer. ip_address must be an existing P-GW ingress peer and be expressed in IPv4 dotted decimal notation.

sgw-egress [ address ip_address ]: Displays information about eGTP-C S-GW egress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW egress peer. ip_address must be an existing S-GW egress peer and be expressed in IPv4 dotted decimal notation.

sgw-ingress [ address ip_address ]: Displays information about eGTP-C S-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW ingress peer. ip_address must be an existing S-GW ingress peer and be expressed in IPv4 dotted decimal notation.
show egtpc peers

| { grep grep_options | more }

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on using the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display information about eGTP-C peers associated with the service interface configured on this system. The output contains the following information about the peer:

- Status of the peer
- Echo status
- Restart counter status
- Peer restart counter knowledge
- Service ID
- Peer IP address
- Current sessions
- Maximum sessions

Important: The primary command, show egtpc peers, when entered without additional keywords, displays information for all peers associated with the service operating on this system.

Example

The following command returns an output for an eGTP-C S-GW egress peers associated with the service interface configured on this system with an IP address of 1.2.3.4:

```
show egtpc peers interface sgw-egress address 1.2.3.4
```

The following command returns an output for an eGTP-C MME peer associated with the service interface configured on this system with an IP address of 1.2.3.4:

```
show egtpc peers interface mme address 1.2.3.4
```
show egtp-service

Displays configuration information for evolved GPRS Tunneling Protocol (eGTP) services on this system.

Product
MME, P-GW, S-GW

Privilege
Inspector

Syntax

```show egtp-service { all | name service_name } [ | { grep grep_options | more } ]```

- `all`
  Displays configuration information for all eGTP services configured on this system.

- `name service_name`
  Displays configuration information for a specific eGTP service configured on this system. `service_name` must be an existing eGTP service, and be from 1 to 63 alpha and/or numeric characters in length.

- `| { grep grep_options | more }`
  Indicates the output of the command is to be piped (sent) to the command specified.
  A command to send output to must be specified.
  For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of Chapter 1 of the Command Line Interface Reference Guide.

Usage
Use this command to view configuration information for eGTP services on this system.

Example
The following command displays service statistics for the eGTP service named `egtp1`:

```show egtp-service name egtp1```
**show egtpc sessions**

Displays eGTP-C session information.

**Product**

MME, P-GW, S-GW

**Privilege**

Inspector

**Syntax**

```
show egtpc sessions [ egtp-service name | interface { mme | pgw-ingress | sgw-egress | sgw-ingress } ] [ | { grep grep_options | more } ]
```

- **egtp-service name**
  
  Displays information about eGTP-C sessions associated with a specific service. *name* must be an existing egtp-service and be from 1 to 63 alpha and/or numeric characters.

- **interface { mme | pgw-ingress | sgw-egress | sgw-ingress }**
  
  Displays information about eGTP-C sessions associated with the service interface configured on this system.
  
  - mme: Displays information about eGTP-C sessions associated with the MME interface configured on this system.
  
  - pgw-ingress: Displays information about eGTP-C sessions associated with the P-GW ingress interface configured on this system.
  
  - sgw-egress: Displays information about eGTP-C sessions associated with the S-GW egress interface configured on this system.
  
  - sgw-ingress: Displays information about eGTP-C sessions associated with the S-GW ingress interface configured on this system.

- **| { grep grep_options | more }**
  
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on using the *grep* and *more* commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display session information for a specific eGTP service or for sessions associated with an interface type configured on this system.

**Example**

The following command displays eGTP-C session information for sessions associated with all P-GW ingress interfaces configured on this system:

```
show egtpc sessions interface pgw-ingress
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:
show egtpc sessions
show egtpc statistics

Displays evolved GPRS Tunneling Protocol Control (eGTP-C) plane statistics for a specific service name or interface type.

Product
MME, P-GW, S-GW

Privilege
Inspector

Syntax
show egtpc statistics [ egtp-service name | interface { mme | pgw-ingress | sgw-egress | sgw-ingress } | mme-address ip_address | pgw-address ip_address | sgw-address ip_address ] [ verbose ] [ | { grep grep_options | more } ]

egtp-service name
Displays statistics for a specific eGTP service configured on this system. service_name must be an existing eGTP service, and be from 1 to 63 alpha and/or numeric characters in length.

interface { mme | pgw-ingress | sgw-egress | sgw-ingress }
mme: Displays eGTP-C statistics for all MME interfaces.
pgw-ingress: Displays eGTP-C statistics for all eGTP P-GW ingress interfaces.
sgw-egress: Displays eGTP-C statistics for all eGTP S-GW egress interfaces.
sgw-ingress: Displays eGTP-C statistics for all eGTP S-GW ingress interfaces.

mme-address ip_address
Displays eGTP-C statistics for a specific MME IP address. ip_address must be an existing MME IP address and be expressed in dotted decimal notation.

pgw-address ip_address
Displays eGTP-C statistics for a specific P-GW IP address. ip_address must be an existing MME IP address and be expressed in dotted decimal notation.

sgw-address ip_address
Displays eGTP-C statistics for a specific S-GW IP address. ip_address must be an existing MME IP address and be expressed in dotted decimal notation.

verbose
Displays the maximum amount of detail available for this command's output. If this option is not specified, the output is truncated to a more concise level.

| { grep grep_options | more }

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on using the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display evolved GPRS Tunneling Protocol Control (eGTPC) plane statistics for a specific service name or interface type.

**Example**

The following command displays eGTPC statistics for interfaces configured as S-GW ingress interfaces:

```
show egtpc statistics interface sgw-ingess
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:

```
show egtpc sessions interface mme
```
show external-inline-servers

This command is obsolete.
show fa-service

Displays information on configured foreign agent services.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show fa-service { all | name fa_name } [ | { grep grep_options | more } ]

all | name fa_name

all: indicates information on all foreign agent services is to be displayed.
name fa_name: indicates only the information for the FA service specified as fa_name is to be displayed.

grep grep_options | more

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 5000 Series Platforms Command Line Interface Reference.

Usage
Display foreign agent service configuration information.

Example
The following commands display information on the FA service sampleService and all services, respectively.

show fa-service name sampleService
show fa-service all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show fans

Displays the current control status, speed, and temperature for the upper and lower fans.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show fans [ | { grep grep_options | more } ]

- grep grep_options | more
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage

View the fan information to verify system hardware status as necessary.

Example

The following command displays information regarding the cooling fans in the system:

  show fans

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show file

Displays the contents of the file specified. The contents are paginated as if it were normal ASCII output.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show file url [ | { grep grep_options | more } ]
```

- **url**
  Specifies the location of a file to display. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats:
  - ASR 5000:
    - `[file:]|[/flash|/pcmcial|/hd]|[/directory]//file_name`
    - `tftp://host[:port]|[/directory]//file_name`
    - `[http: | ftp: | sftp: ]/[/username[:password]]@host[:port]|[/directory]//file_name`

  **Important**: Use of the SMC hard drive is not supported in this release.

- **directory** is the directory name.
- **filename** is the actual file of interest.
- **username** is the user to be authenticated.
- **password** is the password to use for authentication.
- **host** is the IP address or host name of the server.
- **port#** is the logical port number that the communication protocol is to use.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage

Display the contents of files to view such information as log data, trace information, etc.

Example
The following will display the contents of the local file `/pub/log.txt`.

```
show file //pcmcial//pub//log.txt
```
The following command will display the contents of the file `/pub/log.txt` on remote host `remoteABC`.

```
show file ftp://remoteABC/pub/log.txt
```
show firewall flows

This command is obsolete.
show firewall ruledef

This command is obsolete.
show firewall statistics

This command is obsolete.
show freeze-ptmsi imsi

Displays the P-TMSI (packet-temporary mobile subscriber identify) corresponding to the IMSI (international mobile subscriber identity) that has entered a frozen state after the purge timeout timer expires.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show freeze-ptmsi imsi imsi_num
```

- **imsi imsi_num**
  Specifies the IMSI that has been frozen. The first three digits are the MCC (mobile country code). The next two or three digits are the MNC (mobile network code). The remaining digits are the MSIN (mobile station identification number).
  - `imsi_num` Enter a sequence of up to 15 digits.

**Usage**
This command enables the operator to know whether a frozen IMSI has an associated P-TMSI.

**Example**
The following command displays the P-TMSI corresponding to a frozen IMSI:

```
show freeze-ptmsi imsi 262090426000194
```
show ggsn-service

Displays configuration information for GGSN services on the system.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show ggsn-service { all | name ggsn_svc_name} [ | { grep grep_options | more }]

all
Displays information for all GGSN services configured with the given context.

name ggsn_svc_name
Specifies the name of a specific GGSN service for which to display information.
ggsn_svc_name is the name of a configured GGSN service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For more information on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

Usage
This command is used to verify the configuration of one or all GGSN services for monitoring or troubleshooting purposes. The output is a concise listing of GGSN service parameter settings.
If this command is executed from within the local context with the all keyword, information for all GGSN services configured on the system will be displayed.

Example
The following command displays configuration information for a GGSN service called ggsn1:

show ggsn-service name ggsn1
show ggsn-service sgsn-table

This new command is the only way to list all SGSNs by IP address and show the current number of subscribers to each SGSN.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show ggsn-service sgsn-table

Usage
While there are existing commands to show SGSN subscriber information, this new command is the only way to list all SGSNs by IP address and show the current number of subscribers to each SGSN.

Example
The following command will bring up a table showing the current active/inactive status, IP address, reboots/restarts and SGSN users.

show ggsn-service sgsn-table

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show global-title-translation

Displays configuration information for the global title translation (GTT).

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show global-title-translation { address-map name | association name }

address-map name
Displays GTT database. name must be a unique identification comprised of 1 to 63 alphanumeric characters.

association name
Displays GTT association list. name must be a unique identification comprised of 1 to 63 alphanumeric characters.

Usage
This command displays the configuration for the GTT.

Example
The following command displays the address map called gtt-ad1.

show global-title-translation address-map gtt-ad1
show gmm-sm statistics

This command displays statistics for the GPRS Mobility Management and Session Management (GMM/SM) configuration of the system’s SGSN service. GMM/SM supports mobility to allow the SGSN to know the location of a Mobile Station (MS) at any time and to activate, modify and deactivate the PDP sessions required by the MS for user data transfer.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show gmm-sm statistics [ gmm-only | sm-only ] [ gprs-service srvc_name | nsei nse_id | routing-area mcc mcc_id mnc mnc_id lac lac_id rac rac_id ] [ sgsn-service srvc_name | rnc mcc mcc_id mnc mnc_id rnc-id rnc_id | routing area mcc mcc_id mnc mnc_id lac lac_id rac rac_id ] [ verbose ] [ grep grep_options | more ]

gmm-only
Enter this keyword to display only GPRS mobility management (GMM) information for other specified keyword parameters for the current context.

sm-only
Enter this keyword to display only session management (SM) information for other specified keyword parameters for the current context.

gprs-service srvc_name
Enter this keyword to display the statistics for the specified GPRS service. The display request can be narrowed by adding additional keywords.
srvc_name must be an alphanumeric string of 1 to 63 alphanumeric characters.

nsei
Enter this keyword to display the GMM/SM session statistics for the identified network service entity (NSEI).

sgsn-service srvc_name
Enter this keyword to display the statistics for the specified SGSN service. The display request can be narrowed by adding additional keywords.
srvc_name must be an alphanumeric string of 1 to 63 alphanumeric characters.

rnc
Enter this keyword to fine-tune the display of the GMM/SM session statistics just for the specified (rnc-id) radio network controller (RNC).

rnc-id rnc_id
Enter this keyword to identify the specific RNC.
rnc_id must be an integer from 0 through 4095.

**routing-area mcc mcc_id mnc mnc_id lac lac_id rac rac_id**

Enter the **routing-area** keyword to fine-tune the display of the GMM/SM session statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

**mcc mcc_id**

Enter this keyword to specify the mobile country code (MCC) as part of the identification of the RNC or RA. **mcc_id** must be an integer from 100 through 999.

**mnc mnc_id**

Enter this keyword to specify the mobile network code (MNC) as part of the identification of the RNC or RA. **mnc_id** must be an integer from 00 through 999.

**lac lac_id**

Enter this keyword to specify the location area code (LAC) as part of the identification of the RNC or RA. **lac_id** must be an integer from 1 through 65535.

**rac rac_id**

Enter this keyword to specify the routing area code (RAC) as part of the identification of the RNC or RA. **rac_id** must be an integer from 1 through 255.

**verbose**

This keyword displays all possible statistics for specified command or keyword.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For more information on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

**Usage**

Use this command to display usage statistics for the GMM/SM session configurations for SGSN services, including a BSC’s attaches, activations, and throughput.

**Example**

The following command displays GMM/SM statistics for a specific routing area defined for the GPRS service:

```bash
show gmm-sm statistics gprs-service gprs1 routing-area mcc 123 mcc 131 lac 24 rac 11
```

The following command displays all possible information for GMM/SM statistics:

```bash
show gmm-sm statistics verbose
```
show gnm-sm statistics

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gprs-service

Displays the statistics of GPRS service(s) configured in a given context on the system.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gprs-service { all | name gprs_srvc_name } [ | { grep grep_options | more }]
```

- **all**
  Displays information for all GPRS services configured with the given context.

- **name gprs_srvc_name**
  Specifies the name of a specific GPRS service for which information is to be displayed.
  `gprs_srvc_name` is the name of a configured GPRS service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For more information on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

Usage

This command is used to verify the configuration of one or all GPRS services for monitoring or troubleshooting purposes. The output is a concise listing of GPRS service parameter settings.

If this command is executed from within the local context with the all keyword, information for all GPRS services configured on the system will be displayed.

Example

The following command displays configuration information for all GPRS services configured in this context:

```
show gprs-service all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gs-service

Displays configuration information and statistics for Gs service configured on system.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gs-service { all | name svc_name } [ | { grep grep_options | more }]
```

- `all`
  Displays information for all Gs services configured with in the given context.

- `name svc_name`
  Specifies the name of a specific Gs service for which to display information.
  `svc_name` is the name of a configured Gs service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- `grep grep_options | more`
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For more information on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

Usage

This command is used to verify the configuration of one or all Gs services for monitoring or troubleshooting purposes.
If this command is executed from within the local context with the all keyword, information for all Gs services configured on the system will be displayed.

Example

The following command displays configuration information for all Gs services configured on a system:

```
show gs-service all
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gtpc

Displays GTPv0, GTPv1-C, GTPv1-U information with filtering options.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show gtpc [ full | counters | summary ] { all | apn apn_name | imsi imsi_value [ nsap nsapi_value ] | callid callid | sgsn-address ip_address | ggsn-service ggsn_name | user-address ip_address | username username }

[ full | counters | summary ]

Specifies the level of information to be displayed. The following levels can be used:

• **full**: Indicates detailed information is to be displayed.

• **counters**: Indicates the output is to include the statistic counters.

• **summary**: Indicates only summary information is to be displayed.

{ all | apn apn_name | imsi imsi_value [ nsap nsapi_value ] | callid callid | sgsn-address ip_address | ggsn-service ggsn_name | user-address ip_address | username username }

Specifies the filter criteria used when displaying GTP information. The following filters can be used:

• **all**: Specifies that all available information is to be displayed.

• **apn apn_name**: Specifies that GTP information for a particular APN will be displayed. **apn_name** can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

• **imsi imsi_value [ nsap nsapi_value ]**: Specifies that GTP information will be displayed for a particular International Mobile Subscriber Identity (IMSI). **imsi_value** is an integer value from 1 to 15 characters. Optionally, the IMSI could be further filtered by specifying a particular PDP context using the Network Service Access Point Identifier (NSAPI). **nsapi_value** is an integer value from 5 to 15.

• **callid callid**: Specifies that GTP information will be displayed for a particular call identification number. **callid** must be specified as a 4-byte hexadecimal number.

• **sgsn-address ip_address**: Specifies that GTP information for a particular SGSN will be displayed. **ip_address** is the address of the SGSN in dotted decimal notation.

• **ggsn-service ggsn_name**: Specifies that GTP information for a particular GGSN service will be displayed. **ggsn_name** can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

• **user-address ip_address**: Specifies that GTP information for a particular user address will be displayed. **ip_address** is the address of the user’s PDP context in dotted decimal notation.

• **username username**: Specifies that GTP information for a particular username will be displayed. **username** can be from 1 to 127 alpha and/or numeric characters (including wildcards (‘$’ and ‘*’)) and is case sensitive.
Usage

This command displays statistics for every GTP message type based on the filter criteria. This information is useful for system monitoring or troubleshooting.

Example

The following command displays GTPC counters for a GGSN service named ggsn1:

```
show gtpc counters ggsn-service ggsn1
```

The following command displays GTPC full information:

```
show gtpc full
```

The following command displays GTPC summary information for a specific call identification number of 05f62f34:

```
show gtpc summary callid 05f62f34
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show gtpc statistics

Display GTPv0, GTPv1-C, GTPv1-U statistics with filtering options.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gtpc statistics [ apn-name apn_name ] [ custom1 custom2 ] [ sgsn-address address ] [ ggsn-service svc_name ] [ verbose ]
```

- **apn-name apn_name**
  Specifies that GTP statistics for a particular APN will be displayed.
  *apn_name* can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **custom1**
  Displays the statistics of GTP-C messages for preservation mode and free of charge service.
  This keyword is customer-specific license enabled and used for Preservation-Mode and Free-of-Charge Service which are enabled under customer-specific license. For more information on this support, contact your local representative.

- **custom2**
  Displays the statistics of GTP-C messages for overcharging protection on loss of radio coverage for a GGSN service.
  This keyword is feature-specific license enabled and used for subscriber overcharging protection on loss of radio coverage at the GGSN service. For more information on this support, contact your local representative.

- **sgsn-address address**
  Specifies that GTP statistics for a particular SGSN will be displayed.
  *address* is the address of the SGSN in dotted decimal notation.

- **ggsn-service svc_name**
  Specifies that GTP statistics for a particular GGSN service will be displayed.
  *ggsn_name* can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **verbose**
  Specifies that detailed statistics will be displayed.

Usage

The information displayed by this command consists of session statistics such as the number of currently active sessions categorized by PDP context type, and statistics for every GTP message type. The statistics are cumulative.
If the verbose keyword is used, additional information will be displayed such as statistics for every type of error code.

**Example**
The following command displays verbose GTP statistics:

```
show gtpc statistics verbose
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show gtpp accounting

Displays information on the GPRS Tunneling Protocol Prime (GTPP).

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show gtpp accounting servers
```

**Usage**
This command is used to view the status of GTPP accounting servers configured within a context for monitoring or troubleshooting purposes.
If this command is issued from within the local context, a information for all GTPP accounting servers configured on the system is displayed regardless of context.

**Example**
The following command displays the status of and information on configured GTPP accounting servers:

```
show gtpp accounting servers
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gtpp counters

Displays GTPP counters for configured charging gateway functions (CGFs) within the given context.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gtpp counters { all | cgf-address cgf_address }
```

- **all**
  Displays counters for all CGFs configured within the context.

- **cgf-address cgf_address**
  Displays counters for a specific CGF.
  `cgf_address` is the IP address of the CGF expressed in dotted decimal notation.

Usage
Counters for a single CGF can be viewed using the `cgf-address` keyword. Counters for all CGFs in the context can be viewed by entering the command with the `all` keyword.
If this command is issued from within the local context and no CGF-address is specified, the counters displayed will be cumulative for all CGFs configured on the system regardless of context.

Example
The following command displays counters for all CGF:
```
show gtpp counters all
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show gtpp group

Displays information pertaining to the configured GTTP storage server group.

**Product**

GGSN, SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show gtpp group [name gtpp_group_name| all] [ | { grep grep_options| more }]  
```

- **name** gtpp_group_name
  
  Displays information and CDR statistics of the GTTP server group named `gtpp_group_name`. `gtpp_group_name` is name of the configured/default GTTP storage server group.

- **all**
  
  Displays statistics of all configured GTTP storage server group including default group.

- **grep grep_options | more**
  
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  
  For more information on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

**Usage**

Use this command to display the CDR statistics on the basis of GTTP server groups. It shows the information for all or specific GTTP server group configured in the context from which this command is issued.

**Example**

The following command displays the status of the GTTP server group backup server configured in a context called `GTTP_Group1`:

```
show gtpp group name GTTP_Group1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
**show gtp statistics**

Displays GTPP statistics for configured CGFs within the context.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show gtpp statistics [ cgf-address cgf_address ]
```

- **cgf-address cgf_address**
  Specifies the IP address of a specific CGF for which to display statistics and is express in dotted decimal notation.

**Usage**
Statistics for a single CGF can be viewed by specifying its IP address. Statistics for all CGFs in the context can be viewed by not specifying an IP address. If this command is issued from within the local context, the statistics displayed will be cumulative for all CGFs configured on the system regardless of context.

**Example**
The following command displays statistics for a CGF with an IP address of 192.168.1.14:

```
show gtpp statistics cgf-address 192.168.1.14
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gtpp storage-server

Displays information pertaining to the configured GTPP storage server.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show gtpp storage-server [ counters { all | group name } | group name ]
local file { counters { all | group name } | statistics [ group name ] } |
status { verbose } | streaming { counters { all | group name } | statistics [ group name ] } ]
| { grep grep_options | more } |

---

counters
Displays counters for the external GTPP storage server.

---

group name name
Displays GTPP backup server information for the specified group.

---

local file
Displays statistics and counters for the local storage-server. This is the hard disk if hard disk support has been enabled with the gtpp storage-server mode command in the GTPP Group Configuration Mode.

---

statistics
Displays statistics for the GTPP storage server.

---

status { verbose }
Displays status of the GTPP storage server. verbose enables the detailed view.

---

streaming
Displays the status of CDRs backup on HDD while ‘streaming’ mode is enabled.

---

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

---

Usage
Executing this command with no keywords displays status information for the GTPP backup server configured in the context from which this command is issued.
Example

The following command displays the GTPP CDR file statistics stored on the local SMC hard disk.

```
show gtpp storage-server local file counters all
```

The following command displays the status of the GTPP backup server configured in a context called ggsn1:

```
show gtpp storage-server
```

The following command displays statistics for the GTPP backup server configured in a context called ggsn1:

```
show gtpp storage-server statistics
```

The following command displays gtpp storage server counters:

```
show gtpp storage-server counters
```

The following command displays gtpp storage server status:

```
show gtpp storage-server status
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gtpu statistics

Displays GPRS Tunneling Protocol user plane (GTP-U) statistics and counters on this system.

Product
P-GW, S-GW

Privilege
Inspector

Syntax

```
show gtpu statistics [ gtpumgr-instance number ] [ gtpu-service name | peer-address ip_address ]
```

- **gtpumgr-instance number**
  Displays configuration information for a specific GTP-U manager instance.
  *number* must be an existing instance and be an integer value from 1 to 4294967295.

- **gtpu-service name**
  Displays GTP-U statistics and counters for a specific GTP-U service configured on this system.
  *name* must be an existing GTP-U service, and be from 1 to 63 alpha and/or numeric characters in length.

- **peer-address ip_address**
  Displays GTP-U statistics and counters for a specific peer IP address.
  *ip_address* must be an existing peer IPv4 or IPv6 address and be specified in dotted decimal notation (for IPv4) or colon-separated notation (for IPv6).

  | { grep grep_options | more }

  Indicates the output of the command is to be piped (sent) to the command specified.
  A command to send output to must be specified.
  For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of Chapter 1 of the Command Line Interface Reference Guide.

Usage

Use this command to view statistics and counters for GTP-U traffic on this system.

Example

The following command displays statistics for the GTP-U service named *egtp1*:

```
show egtpu statistics gtpu-service egtp1
```
show gtpu-service

Displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services on this system.

Product
P-GW, S-GW

Privilege
Inspector

Syntax

show gtpu-service { all | name service_name } [ | { grep grep_options | more } ]

all
Displays configuration information for all GTP-U services configured on this system.

name service_name
Displays configuration information for a specific GTP-U service configured on this system.

service_name must be an existing GTP-U service, and be from 1 to 63 alpha and/or numeric characters in length.

| { grep grep_options | more }
Indicates the output of the command is to be piped (sent) to the command specified.
A command to send output to must be specified.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of Chapter 1 of the Command Line Interface Reference Guide.

Usage
Use this command to view configuration information for GTP-U services on this system.

Example
The following command displays service statistics for the GTP-U service named egtpl:

show egtpl-service name egtpl
Chapter 94
Exec Modes Show Commands (H-L)

This section includes the commands `show ha-service` through `show logs`.
show ha-service

Displays information on configured home agent services.

Product
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ha-service { all | name ha_name } [ | { grep grep_options | more } ]
```

- **all | name ha_name**
  - `all`: indicates information on all home agent services is to be displayed.
  - `name ha_name`: indicates only the information for the HA service specified as `ha_name` is to be displayed.

- **grep grep_options | more**
  - Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage
Display home agent service configuration information.

Example
The following commands displays information on the HA service `sampleService` and all services, respectively.

```
show ha-service name sampleService show ha-service all
```
show hardware

Displays information on the system hardware.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show hardware ( card [ card_num ] | inventory | version [ board | diags | fans ] ) [ | { grep grep_options | more } ]
```

- **card [ card_num ]**
  - Provide the hardware information for all cards or the card specified by `card_num`. `card_num` must be a value in the range 1 through 48 and must refer to an installed card.

- **inventory**
  - Display the hardware information for all slots in tabular format.

- **version [ board | diags | fans ]**
  - Display the CPU information for all application cards and fan controller version for the upper and lower fan trays.
    - **board**: Only include the CPLD and FPGA version information.
    - **diags**: Only include the CFE diagnostics version information.
    - **fans**: Show the fan controller versions for the upper and lower fan trays.

- **grep grep_options | more**
  - Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Show the hardware information to verify part lists and hardware component versions with reserve stock.

Example

The following displays the hardware information for a card installed in slot 1.

```
show hardware card 1
```

The following command displays the hardware inventory for the entire chassis.

```
show hardware inventory
```
The following command results in the display of the CPU version for all application cards displaying only the CPLD and FPGA information.

```
show hardware version board
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show hd raid

Shows the output of the RAID established on the ASR 5000 SMCs.

Product
All

Privilege
Security Administrator, Administrator, Administrator, Operator

Syntax

show hd raid [ verbose ]

Example

show hd raid verbose

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show hd-storage-policy

Displays ACR counter and statistic information.

Product
HSGW, P-GW, S-GW

Privilege
Inspector

Syntax

show hd-storage-policy { all | counters [ all ] [ name name ] [ verbose ] | name name | statistics [ all ] [ name name ] [ verbose ] }

- **all**
  Specifies that ACR information for all HD storage policies configured on the system is to be displayed.

- **counters [ all ] [ name name ] [ verbose ]**
  Specifies that ACR counter information for HD storage policies configured on the system is to be displayed.

- **name name**
  Specifies that ACR information for an HD storage policy with the specified name is to be displayed.

- **statistics [ all ] [ name name ] [ verbose ]**
  Specifies that ACR statistic information for HD storage policies configured on the system is to be displayed.

- **verbose**
  Displays HD storage statistics based on instance.

Usage

Use this command to display ACR counter and statistic information.

Example

The following command displays ACR statistic information for an HD storage policy named pgwsgw:

```
show hd-storage-policy statistics name pgwsgw
```
show hnbgw counters

This command displays the session counter information for Home-NodeB Gateway (HNB-GW) services and HNBs connected on this system.

**Product**
HNB-GW

**Privilege**
Inspector

**Syntax**

```
show hnbgw counters [hnbgw-service service_name | hnbid hnb_identifier] [ | { grep grep_options | more }]  
```

- **hnbgw-service service_name**
  - This keyword is used to filter the counter display based on the HNB-GW service name `service_name` configured and running on this system.
  - `service_name` must be an existing HNB-GW service, and be from 1 to 63 alpha and/or numeric characters in length.

- **hnbid hnb_identifier**
  - This keyword is used to filter the counter display based on Home-NodeB `hnb_identifier` which is connected to this system with HNB-GW service and in active or dormant state.
  - `hnb_identifier` must be an identifier for HNB from 1 to 255 alpha and/or numeric characters in length.

- `| { grep grep_options | more }
  - Indicates the output of the command is to be piped (sent) to the command specified.
  - A command to send output to must be specified.
  - For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter of the Command Line Interface Reference.

**Usage**

Use this command to view the session counter information for HNB-GW services configured and HNBs connected on this system.

**Example**

The following command displays the counters for the HNB-GW service named `hnbgw1`:

```
show hnbgw counter hnbgw-service hnbgw1
```
show hnbgw statistics hnbgw-service

This command displays the session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

**Product**
HNB-GW

**Privilege**
Inspector

**Syntax**

```
show hnbgw statistics hnbgw-service service_name [hnbap-only | ranap-only | rua-only | sccp-only | sctp-only] [ verbose] [ grep grep_options | more ]
```

**hnbgw-service service_name**

This keyword is used to filter the session statistics display based on the HNB-GW service name `service_name` configured and running on this system. `service_name` must be an existing HNB-GW service, and be from 1 to 63 alpha and/or numeric characters in length.

**hnbap-only**

This keyword is used to filter the session statistics display limited to Home NodeB Application Part (HNBAP) traffic only for selected HNB-GW service which is configured and running on this system.

**ranap-only**

This keyword is used to filter the session statistics display limited to Radio Access Network Application Protocol (RANAP) traffic only for selected HNB-GW service which is configured and running on this system.

**rua-only**

This keyword is used to filter the session statistics display limited to RANAP User Adaptation (RUA) traffic only for selected HNB-GW service which is configured and running on this system.

**sccp-only**

This keyword is used to filter the session statistics display limited to Signaling Connection Control Part (SCCP) traffic only for selected HNB-GW service which is configured and running on this system.

**sctp-only**

This keyword is used to filter the session statistics display limited to Stream Control Transmission Protocol (SCTP) traffic only for selected HNB-GW service which is configured and running on this system.

**verbose**

This keyword is used to display the detailed statistics for all sessions on HNB-GW services or for selected filter and named HNB-GW service which is configured and running on this system.
Indicates the output of the command is to be piped (sent) to the command specified.
A command to send output to must be specified.
For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter of the Command Line Interface Reference.

Usage
Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

Example
The following command displays the session statistics for HNBAP part of session details for the HNB-GW service named `hnbwl`:

```
show hnbgw statistics hnbgw-service hnbwl hnbap-only
```

The following command displays the session statistics for RANAP part of session with maximum details for the HNB-GW service named `hnbwl`:

```
show hnbgw statistics hnbgw-service hnbwl ranap-only verbose
```
show hnbgw statistics hnbid

This command displays the session statistics for Home-NodeB (HNB) connected to an HNB-GW service on this system.

| Product | HNB-GW |
| Privilege | Inspector |

Syntax

```
show hnbgw statistics hnbid hnb_identifier[hnbp-only | ranap-only | rua-only] [ verbose] [ | { grep grep_options | more } ]
```

```
hnbid hnb_identifier
```

This keyword is used to filter the session statistics display based on Home-NodeB `hnb_identifier` which is connected to this system through an HNB-GW service. `hnb_identifier` must be an identifier for HNB from 1 to 255 alpha and/or numeric characters in length.

```
hnbap-only
```

This keyword is used to filter the session statistics display limited to Home NodeB Application Part (HNBAP) traffic only for selected HNB which is connected to this system through HNB-GW service.

```
rana-only
```

This keyword is used to filter the session statistics display limited to Radio Access Network Application Protocol (RANAP) traffic only for selected HNB which is connected to this system through HNB-GW service.

```
rua-only
```

This keyword is used to filter the session statistics display limited to RANAP User Adaptation (RUA) traffic only for selected HNB which is connected to this system through HNB-GW service.

```
verbose
```

This keyword is used to display the detailed statistics for all HNB sessions or for selected filter and HNB which is connected to this system through HNB-GW service.

```
| { grep grep_options | more }
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of the `grep` and `more` commands, refer to the `Regulating a Command’s Output` section in `Command Line Interface Overview` chapter of the `Command Line Interface Reference`.

Usage

Use this command to view the session statistics for overall session or in selected part of user session for selected HNB which is connected to this system through HNB-GW service.
Example
The following command displays the session statistics for HNBAP part of session details for the HNB having
hnbl12234 as identifier on this system:

    show hnbgw statistics hnbid hnb112234 hnbap-only

The following command displays the detailed session statistics for RANAP part of session details for the HNB having
hnbl12234 as identifier on this system:

    show hnbgw statistics hnbid hnb112234 ranap-only verbose
show hnbgw-service

This command displays the configuration details for configured HNB-GW service(s) on this system.

Product
HNB-GW

Privilege
Inspector

Syntax

show hnbgw-service {all | hnbgw-service service_name}

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>This keyword is used to display the configuration and other default parameters for all HNB-GW service configured on this system.</td>
</tr>
<tr>
<td>hnbgw-service service_name</td>
<td>This keyword displays the configuration and default parameters for specific HNB-GW service name service_name which is configured and running on this system. Service_name must be an existing HNB-GW service, and be from 1 to 63 alpha and/or numeric characters in length.</td>
</tr>
</tbody>
</table>

Usage

Use this command to view the configuration and service parameters set for all or any specific HNB-GW service(s) on this system.

Example

The following command displays the configured and default parameters for all HNB-GW services configured on this system:

```
show hnbgw-service all
```
show hsgw-service

Displays configuration information for HRPD Serving Gateway (HSGW) services on this system.

**Product**
HSGW

**Privilege**
Inspector

**Syntax**

```
show hsgw-service { all | name service_name } [ | { grep grep_options | more } ]
```

| all |
| Displays configuration information for all HSGW services configured on this system.

| name service_name |
| Displays configuration information for a specific HSGW service configured on this system. service_name must be an existing HSGW service, and be from 1 to 63 alpha and/or numeric characters in length.

| [ | { grep grep_options | more } |
| Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command’s Output section of Chapter 1 of the Command Line Interface Reference Guide.

**Usage**

Use this command to view configuration information for HSGW services on this system.

**Example**

The following command displays service statistics for the HSGW service named **hsgw1**:

```
show hsgw-service name hsgw1
```
show ims-authorization policy-control

Displays information and statistics specific to the policy control in IP Multimedia Subsystem (IMS) authorization service.

**Product**
SCM, GGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show ims-authorization policy-control statistics [ service ims_auth_svc_name ]
server { ip-address ip_address [ port port_value ] | name server_name } ] [ ] {
grep grep_options | more } ]
```

**statistics**
Displays the total collected statistics of all policy control parameters of IMS authorization service sessions since the last system restart or clear command.

**service ims_auth_svc_name**
Displays the total collected statistics of all IMS authorization sessions processed by a specific IMS authorization service since the last system restart or clear command. `ims_auth_svc_name` must be an existing IMS authorization service name.

**server { ip-address ip_address [ port port_value ] | name server_name }**
Displays the server-level message statistics and the server IP address. Specify the PCRF server IP address or server name.

**grep grep_options | more**
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
Use this command to display information and statistics about policy control configuration in existing IMS authorization services.

**Example**
The following command displays the existing IMS authorization service name `ims_auth_gxl` on the system:

```
show ims-authorization policy-control statistics service ims_auth_gxl
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show ims-authorization policy-control
show ims-authorization policy-gate

Displays information of installed Policy Gates for specific subscriber in IP Multimedia Subsystem (IMS) authorization service.

Product
SCM, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ims-authorization policy-gate { { status [ summary | full ] [ { imsi imsi_value [ nsapi nsapi_value ] | callid call_id [ { ims-auth-service ims_auth_svc } [ rulename rule_name ] ] | { counters [ all | { imsi imsi_value [ nsapi nsapi_value ] | { rulename rule_name } | { callid call_id } ] } [ grep grep_options | more ] } ] ]

status [ summary | full ]
This option displays the status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified criteria.
summary: limits the display to a summary on status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based.
full: displays the full information on status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based.

counters all
This option displays the counters/statistics of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified criteria.
all displays the all counters of the installed gates and their flow definitions along with the run-time status in an IMS authorization service based.

imsi imsi_value [ nsapi nsapi_value ]
This option displays all of the counters/status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified International Mobile Subscriber Identity (IMSI) named imsi_value.
nsapi nsapi_value specifies Network Service Access Point Identifier (NSAPI) named nsapi_value to limit the display to a single PDP context of the subscriber.

callid call_id
This option displays all of the counters/status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified call identifier named call_id.

ims-auth-service ims_auth_svc
This option displays status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service named ims_auth_svc.
```
show ims-authorization policy-gate

**rulename** rule_name

This option displays all of the counters/status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specific dynamic charging rule named rule_name.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. Please refer to the Regulating a Command’s Output section of the Command Line Interface Reference for details on the usage of grep and more.

**Usage**

Use this command to display information/statistics/counters about all of the installed policy gates and their flow definitions along with the run-time status with specified criteria and filters in existing IMS authorization services.

**Example**

The following command displays the full status of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate status full
```

The following command displays all counters of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate counters all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show ims-authorization servers

Displays information and statistics specific to the authorization servers used for IP Multimedia Subsystem (IMS) authorization service.

Product
SCM, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
show ims-authorization servers [ ims-auth-service ims_auth_svc_name [ | { grep grep_options | more } ] ]
```

```
server [ ims-auth-service ims_auth_svc_name ]
```
Displays the information and statistics of all authorization servers configured for IMS authorization service in a system.
ims-auth-service ims_auth_svc_name: Displays the configured authorization servers for IMS authorization for an IMS authorization service named ms_auth_svc_name.

```
grep grep_options | more
```
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
Please refer to the Regulating a Command’s Output section of the Command Line Interface Reference for details on the usage of `grep` and `more`.

Usage
Use this command to display information and statistics about IMS authorization servers configured on a system or IMS authorization service.

Example
The following command displays the information and statistics of the authorization servers in IMS authorization service named `ims_auth_gxl`:

```
show ims-authorization servers ims-auth-service ims_auth_gxl
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show ims-authorization service

Displays information, configuration, and statistics of all/specific IP Multimedia Subsytem (IMS) authorization service.

Product
SCM, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
show ims-authorization service { { all [ verbose ] | name ims_auth_svc_name | summary } } | { statistics [ all | name ims_auth_svc_name ] [ verbose ] } [ | { grep grep_options | more } ]
```

**all [ verbose ]**
Displays information and configuration of all configured IMS authorization services with a single line of information for each IMS authorization service.
verbose: Displays all information and configuration data of every IMS authorization services configured on system.

**name ims_auth_svc_name**
Displays the information, statistics, and configuration data of an IMS authorization service named ims_auth_svc_name.

**summary**
Displays summarized information and configuration data of all IMS authorization services configured in a system.

**statistics [ all | name ims_auth_svc_name ] [ verbose ]**
Displays the IMS Authorization service statistics including following information:
- Initial authorization procedures
- Re-authorization procedures initiated by us
- Re-authorization procedures initiated by servers
- Various failure statistics

If no criteria specified summarized statistics of all IMS Authorization services are displayed
- **all**: displays individual statistics for every IMS authorization service configured on system.
- **name ims_auth_svc_name**: Displays the statistics of the IMS authorization service named ims_auth_svc_name
- **verbose**: displays the detailed statistics of a configured IMS authorization service.

**grep grep_options | more**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
show ims-authorization service

Please refer to the Regulating a Command’s Output section of the Command Line Interface Reference for details on the usage of `grep` and `more`.

Usage

Use this command to display the IMS Authorization service status, counters and configuration. The status includes the state of a server table switchover. Statistics option is used for various processes and procedure status.

Example

The following command displays the information and configuration data of the IMS authorization service named `ims_auth_gxl`:

```
show ims-authorization service name ims_auth_gxl
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show ims-authorization sessions

Displays information, configuration, and statistics of sessions active in IP Multimedia Subsystem (IMS) authorization service.

Product
SCM, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
show ims-authorization session [ full | summary ] | [ all ] | [ ims-auth-service ims_auth_svc_name | imsi imsi_value [ nsapi nsapi_value ] | apn apn_name | ip-address ip_address | callid call_id ] [ | { grep grep_options } more ]
```

**full**
Displays complete information and configuration data of all sessions in IMS authorization services configured in a system.

**summary**
Displays summarized information and configuration data of all sessions in IMS authorization services configured in a system.

**all**
Displays information and configuration of all sessions running in IMS authorization services with a single line of information for each IMS authorization session.

**ims-auth-service ims_auth_svc_name**
Displays the information, statistics, and configuration data of sessions in an IMS authorization service named ms_auth_svc_name.

**imsi imsi_value [ nsapi nsapi_value ]**
This option displays all of the counters/status of the running services in an IMS authorization service based on the specified International Mobile Subscriber Identity (IMSI) named imsi_value. The option **nsapi nsapi_value** specifies Network Service Access Point Identifier (NSAPI) named nsapi_value to limit the display to a single PDP context of the subscriber.

**apn apn_name**
This option displays all of the counters/status of the running services in IMS authorization service based on the access point name (APN) named apn_name.

**ip-address ip_address**
This option displays all of the counters/status of the running services in IMS authorization service based on the host IP address having IP address value as ip_address.
show ims-authorization sessions

**callid call_id**
This option displays all of the counters/status of the running services in IMS authorization service based on the specified call identifier named `call_id`.

**summary**
Displays summarized information and configuration data of all IMS authorization services configured in a system.

**grep grep_options | more**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. Please refer to the Regulating a Command’s Output section of the Command Line Interface Reference for details on the usage of `grep` and `more`.

**Usage**
Use this command to display the sessions running under IMS Authorization service on a system with different filter criteria.

**Example**
The following command displays the information and statistical data of a session in IMS authorization service:

```bash
show ims-authorization sessions full
```

**Important**: Output descriptions for commands are available in the Statistics and Counters Reference.
show ip

Displays information for the IP-based interfaces’ access group and access list information along with address resolve protocol information for the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ip { access-group [ statistics] | access-list [ list_name ] | arp [ arp_ip_address ] | [summary] | statistics ] | localhost [ host_name ] | prefix-list [ detail [list_name ] | namelist_name | summary [list_name ] ] | rip | route [route_ip_address [route_gw_address ] ] | static-routes [route_ip_address [ sroute_gw_address ] | vrf vrf-name] [ | { grep | grep_options | more }]
```

<table>
<thead>
<tr>
<th>access-group [ statistics ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays all configured access groups in the current context along with the priority values.</td>
</tr>
<tr>
<td>statistics: Displays all configured access groups along with packet and byte counters for each ACL rule hit for the current context. In addition, it shows the priority values.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>access-list [ list_name ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates the output is to display the information for all access control lists or the list specified as list_name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>arp [ arp_ip_address ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the address resolution protocol table or the ARP information associated with the IP address specified as $(arp_ip_address). $(arp_ip_address) must be specified using the standard IPv4 dotted decimal notation.</td>
</tr>
</tbody>
</table>

**Important:** When the VPN Manager restarts, it removes all interfaces from the kernel and thus the kernel removes all ARP entries. When this happens, the NPU still holds all of the ARP entries so that there is no traffic disruption. When this happens, from a user point of view, `show ip arp` is broken since this command gathers information from the Kernel and not the NPU.

<table>
<thead>
<tr>
<th>localhost [ host_name ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays all the local host information or only for the host specified as host_name.</td>
</tr>
</tbody>
</table>

| prefix-list [ detail [list_name ] | name list_name | summary [list_name ] ] |
|---------------------------|
| This keyword list information on configured IP prefix lists. With no keyword supplied, a list of all prefix lists and their entries is displayed. |
| detail [list_name]: Lists detailed information for all prefix lists and their entries. If a list name is specified only the details for the specified prefix list are displayed. list_name must be a string of from 1 through 79 alpha and/or numeric characters. |
**show ip**

**name list_name**: Lists the entries for a specified prefix list. *list_name* must be a string of from 1 through 79 alpha and/or numeric characters.

**summary [ list_name ]**: Lists summary information for all prefix lists and their entries. If a list name is specified only the summary for the specified prefix list are displayed. *list_name* must be a string of from 1 through 79 alpha and/or numeric characters.

---

**rip**

Displays general RIP routing process information. (RIP is not supported at this time.)

**route [ route_ip_address [ route_gw_address ] ]**

Indicates the route information to the address specified by *route_ip_address* is to be displayed. The route gateway address may be specified as needed to identify the route. *route_ip_address* and *route_gw_address* must be specified using the standard IPv4 dotted decimal notation.

**static-route sroute_ip_address [ sroute_gw_address ]**

Displays the static route information for the address specified by *sroute_ip_address* is to be displayed. The static route gateway address may also be specified to identify the route. *sroute_ip_address* and *sroute_gw_address* must be specified using the standard IPv4 dotted decimal notation.

**vrf vrf_name**

Displays the routing information of the VRF. *vrf_name* is a name used to identify a VRF.

**grep grep_options | more**

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

**Usage**

Show the IP information to verify and/or troubleshooting communication difficulties between to a remote host/node.

**Example**

The following command displays the ACL for the list named *sampleACL*.

```bash
show ip access-list sampleACL
```

The following command will output the static route information to remote host 1.2.3.4.

```bash
show ip static-route 1.2.3.4
```
show ip as-path-access-list

Displays the contents of a BGP router AS path access list in the current context.

**Product**
HA

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show ip as-path-access-list list_name
```

- **list_name**
  The name of an existing AS path access list configured in the current context. must be an alpha and or numeric string from 1 through 79 characters in length.

**Usage**
Use this command to display the configured entries for the specified BGP router AS path access list in the current context.

**Example**
The following command displays the contents of an AS path access list named ASlist1:

```
show ip as-path-access-list ASlist1
```
show ip bgp

Displays BGP information for the current context.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ip bgp [ip_address/mask] debugging | filter-list list_name | neighbors [ip_address] | route-map map_name| vpn4 { all [network | neighbors | summary ] | vrf vrf-name [ network ] | route-distinguisher [ network | neighbors | summary ] } [ | { grep grep_options | more } ]
```

**ip_address/mask**

Specify the IP address and netmask bits for the network for which information should be displayed. *ip_address* is an IPv4 address in dotted-decimal notation and *mask* is the number of subnet bits, representing a subnet mask in shorthand. These must be entered in the dotted-decimal notation/subnet bits format (1.1.1.1/24).

**debugging**

Display debug flags that are enabled.

**filter-list list_name**

Display routes that match the specified filter list.

**neighbors [ip_address]**

Display information for all neighbors or a specified neighbor. *ip_address* is an IPv4 address in dotted-decimal notation.

**route-map map_name**

Display routes that match the specified route-map.

**vpn4 { all [network | neighbors | summary ] | vrf vrf-name [ network ] | route-distinguisher [ network | neighbors | summary ] }**

Display all VPNv4 routing data, routing data for a VRF, or a route-distinguisher.

- **all**: displays all VPN routing information. If this is specified, the information displayed is gathered from all the VRF's known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network.
- **network**: displays the network for which information in the BGP routing table.
- **neighbors**: shows neighbor information for the all the vrf with the matching RD value.
- **summary**: shows summary information of neighbors for all the vrf with the matching RD value.
**vrf vrf name**: name used to identify a VRF. Information is only gathered from the corresponding VRF. If there is no such VRF, an error is reported.

**network**: displays the network for which information in the BGP routing table.

**route-distinguisher**: If specified along with the RD value, the information displayed is gathered from the corresponding VRF whose RD value is the same as the specified value. If there is no VRF associated with such an RD, an error is reported.

**network**: displays the network for which information in the BGP routing table.

**neighbors**: shows neighbor information for all the vrf's including the default vrf or for the VRF with a matching RD value.

**summary**: shows summary information of neighbors for all the vrf's including the default vrf or for the VRF with a matching RD value.

```
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter in the `Command Line Interface Reference`.

**Usage**

Use this command display to BGP information for the current context.

**Example**

The following command displays information for all BGP neighbors:

```
show ip bgp neighbors
```
show ip interface

This command displays the statistical and configuration information for the IP-based interfaces including VRF table for specific context.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show ip interface [vrf vrf-name] [ name intfc_name [statistics] [tunnel [gre-keepalive ] ] [summary] [ | (grep grep_options | more ) ]
```

- **vrf vrf-name**
  Displays the routing information of the VRF. `vrf_name` is a name used to identify a VRF.

- **name intfc_name**
  Indicates the name of the interface for which information has to be displayed. If no interface name is specified then information for all IP interfaces is displayed.
  `intfc_name` is name of the configured IP interface.

- **tunnel [ gre-keepalive ]**
  This keyword will filter the IP interface information for tunnel type of interfaces.
  It is applicable for GRE/IP-in-IP type of tunnel interfaces only.
  `gre-keepalive`: This optional keyword displays the GRE keepalive information for GRE tunnel configured with this IP interface.

- **statistics**
  Displays the session statistics of all ingress and egress packets processed through this IP interface.

- **summary**
  Displays summarized information about requested IP interface/s.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to display the summarized of detailed configuration and statistical information for configured IP interface. This information can be used to verify and/or troubleshooting communication difficulties between to a remote host/node.
Example
The following command displays the interface information, including statistics, for the IP interface `sampleInterface`.

```
show ip interface sampleInterface statistics
```

The following command displays the GRE keepalive information for an IP interface named `IP_grel`.

```
show ip interface IP_grel tunnel gre-keepalive
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show ip ospf

This command displays OSPF routing information.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show ip ospf [ border-routers | database [ verbose ] [ ls-id ip_addr ] [ adv-router ip_addr ] [ ls-type { router | network | summary | asbr-summary | external | nssa [integer] } ] [ debugging | interface | neighbor [ details ] | route | virtual-links ]
```

- `border-routers`
  Displays all known area border routers (ABRs) and Autonomous System border routers (ASBRs) for OSPF.

- `database [ verbose ] [ ls-id ip_addr ] [ adv-router ip_addr ] [ ls-type { router | network | summary | asbr-summary | external | nssa [integer] } ]`
  Displays a summary of the database information for OSPF.

  - `verbose`: Display detailed OSPF database information.
  - `ls-id ip_addr`: Display OSPF database information for the LSAs with the specified LSID.
  - `adv-router ip_addr`: Display OSPF database information for the advertising router with the specified LSID.
  - `ls-type { router | network | summary | asbr-summary | external | nssa [integer] }`: Display OSPF database information for the specified LSA type.

- `debugging`
  Lists which debugging parameters are enabled.

- `interface`
  Displays interface information for OSPF.

- `neighbor [ details ]`
  Displays summary information about all known OSPF neighbors.

  - `details`: Displays detailed information about all known OSPF neighbors.

- `route [ summary ]`
  Displays the OSPF routing table.

  - `summary`: Displays the number of intra-area, inter-area, external-1 and external-2 routes.

- `virtual-links`
  Displays the OSPF virtual links.
show ip ospf

Usage
Use this command to display OSPF information.

Example
To display general OSPF information, enter the following command;

    show ip ospf
show ip policy-forward

Displays information for IP packet redirecting policy for HA.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show ip policy-forward
```

**Usage**

Use this command to see all the settings for IP packet redirection configuration from existing HA to new HA during upgrade.

**Important:** It is a customer specific command.

**Example**

The following command displays forward policy configuration for an HA:

```
show ip policy-forward
```
show ip pool

This command displays statistics specific to IP pools.

Product
PDSN, GGSN, HA, ASN-GW, A-BG

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show ip pool [ address {pool-name pool_name | group-name group_name} {used | free | hold | release} [limit limit]] | group-name group_name | groups | hold-timer {imsi imsi | msid msid | username username [imsi imsi | msid msid] } | overlap | pool-name pool_name | private | public | resource | static | summary | verbose | wide ]

address {pool-name pool_name | group-name group_name} {used | free | hold | release} [limit limit]
Displays IP pool addresses for the specified IP pool or pool group that are currently in the specified state.

pool-name pool_name: Show IP addresses from the IP pool with the specified name. pool_name must be the name of an existing IP pool.

group-name group_name: Show IP addresses from the IP pool group with the specified name. group_name must be the name of an existing IP pool group.

used: Display the IP addresses that are in a used state.
free: Display the IP addresses that are in a free state.
hold: Display the IP addresses that are in a hold state.
release: Display the IP addresses that are in a release state.
limit limit: The maximum number of address to display. limit must be an integer from 1 through 524287.

group-name group_name
Show information about the IP pool group with the specified name. group_name must be the name of an existing IP pool group.

groups
List information about all IP pool groups.

hold-timer {imsi imsi | msid msid | username username [imsi imsi | msid msid]}
Displays hold timer address information for the specified IMSI, MSID, or username.

imsi imsi: The IMSI for which to display hold-timer information. imsi must be a valid IMSI (International Mobile Subscriber Identity) ID which is a 15 character field that identifies the subscriber’s home country and carrier.

msid msid: The MSID for which to display hold-timer information. msid must be a mobile subscriber ID from 7 through 16 digits.

username username: The username for which to display hold-timer information. username must be an alpha and or numeric string of from 1 through 127 characters.
**Important:** Active users cannot be displayed. If an active ID or username is entered, the following error message appears: Failure: No address matching the specified information was found! Please confirm that the options used match the network architecture/deployment, i.e. IMSI/MSID only, Username only, or IMSI/MSID plus Username. Please note that this command does not apply for addresses in the used state.

**overlap**
List information on overlapping IP pools

**pool-name pool_name**
Show information about the specified IP pool. *pool_name* must be the name of an existing IP pool.

**private**
Show information about IP pools marked private.

**public**
Show information about IP pools marked public.

**resource**
Show information about resource IP pools.

**static**
Show information about static IP pools.

**summary**
Show a summary of all IP pool information.

**verbose**
Show detailed information about all IP pools.

**wide**
Show detailed information formatted to more than 80 columns.

**grep grep_options | more**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**
Use this command to display statistics pertaining to IP Pools in the current context.

**Example**
The following command displays IP address information for an IP Pool named *pool1*:
show ip pool address pool-name pool

To display a summary list for all IP pools in the current context, enter the following command:

show ip pool summary

The following command displays IP pool information for all IP pools configured in the current context:

show ip pool verbose

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show ip ipsp

Displays the names of IP pools that are enabled for the IP pool sharing protocol (IPSP) and lists the disposition of addresses in the pools.

Product
PDSN, HA, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
showipipsp [ summary ]
```

<table>
<thead>
<tr>
<th>summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only show the disposition of the addresses in the participating IP pools. Do not show the names of the participating IP pools.</td>
</tr>
</tbody>
</table>

Usage
Use this command to list the names of IP pools that are participating in the IPSP and list the disposition of IP addresses in those pools.

Important: For information on configuring and using IPSP refer to the System Administration and Configuration Guide.

Example
To list information on all IPSP participating pools and address disposition, enter the following command:

```
show ip ipsp
```
show ipms status

Displays the status of IPMS client service with information related to system and call events. It also displays the status of IPMS servers configured.

Product
IPMS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show ipms status [summary | all | server address ip_address]

---

summary
Displays the summary of all configured IPMS client and IPMS servers.

all
Displays information for all configured IPMS client and IPMS servers.

server address ip_address
Displays status for a specific IPMS server.
ip_address is the IP address of the desired IPMS server and must be entered in IPv4 dotted decimal notation.

---

Usage
This command is used to show/verify the status or configuration of one or all IPMS server along with system and call event information.

Example
The following command displays status of an IPMS server with IP address 1.2.3.4:

show ipms status server address 1.2.3.4
**show ipsg**

Displays information and statistics specific to the IP Services Gateway service.

**Product**

IPSG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```bash
show ipsg { service { all [ counters ] | name name } | sessions { all | callid num | counters { criteria } | full { criteria } | ip-address address | msid num | peer-address address | summary { criteria } | username name } | statistics [ name name | peer-address address ] } [ | { grep grep_options| more } ]
```

- **service { all [ counters ] | name name }**
  - Displays information about the configured IPSG service.
  - `all [ counters ]`: Displays information about all of the configured IPSG services on the system.
  - `name name`: Displays information about a specific IPSG service on the system. `name` must be an existing IPSG service name.

- **sessions { all | callid num | counters { criteria } | full { criteria } | ip-address address | msid num | peer-address address | summary { criteria } | username name }**
  - `all`: Displays session information including call ID, NAI, and home address for all current IPSG sessions. This is the default behavior for the `sessions` keyword.
  - `callid num`: Displays session information for a current IPSG session based on the call ID. `num` must be an existing IPSG service session call ID.
  - `counters { criteria }`: Displays session counters for sessions matching the criteria. (See `criteria` below.)
  - `full { criteria }`: Displays all available session information for sessions matching the criteria. (See `criteria` below.)
  - `ip-address address`: Displays session information for a current IPSG session based on the MSID. `num` must be an existing IPSG service session MSID.
  - `msid num`: Displays session information for a current IPSG session based on the IP address of the device sending the RADIUS accounting messages. `address` must be an existing IPSG service session IP address for the device sending the RADIUS accounting messages.
  - `peer-address address`: Displays session information for a current IPSG session based on the IP address of the subscriber. `address` must be an existing IPSG service session subscriber IP address.
  - `summary { criteria }`: Displays a summary of available session information for sessions matching the criteria. (See `criteria` below.)
  - `username name`: Displays session information for a specific IPSG session based on the username of the subscriber. `name` must be an existing IPSG service session subscriber username.

- **statistics [ name name | peer-address address ]**
  - `name name`: Displays session information for all existing IPSG service sessions.
  - `peer-address address`: Displays session information for a specific IPSG session based on the call ID. `num` must be an existing IPSG service session call ID.

- **counters { criteria }**

- **full { criteria }**

- **ip-address address**

- **msid num**

- **peer-address address**

- **summary { criteria }**

- **username name**

- **callid num**

- **all**

- **counters { criteria }**

- **full { criteria }**

- **ip-address address**

- **msid num**

- **peer-address address**

- **summary { criteria }**

- **username name**
show ipsg

**msid num**: Displays session information for a specific IPSG session based on the MSID. _num_ must be an existing IPSG service session MSID.

**peer-address address**: Displays session information for a current IPSG session based on the IP address of the device sending the RADIUS accounting messages. _address_ must be an existing IPSG service session IP address for the device sending the RADIUS accounting messages.

**username name**: Displays session information for a specific IPSG session based on the username of the subscriber. _name_ must be an existing IPSG service session subscriber username.

**statistics [ name name | peer-address address ]**: Displays the total collected statistics of all IPSG sessions since the last system restart or clear command.

- **name name**: Displays the total collected statistics of all IPSG sessions processed by a specific service since the last system restart or clear command. _name_ must be an existing IPSG service name.
- **peer-address address**: Displays the total collected statistics of all IPSG sessions associated with a specific IP address of the device responsible for sending the RADIUS accounting messages. Displayed statistics are from the last system restart or clear command.

**grep grep_options | more**: Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.

For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

Use this command to display information and statistics about existing IPSG services.

**Example**

The following command displays the existing IPSG services on the system:

```
show ipsg service all
```

The following command displays all the existing IPSG service sessions on the system:

```
show ipsg session all
```

The following command displays the cumulative IPSG session statistics on the system:

```
show ipsg statistics
```

The following command displays the cumulative IPSG session statistics on the system for an IPSG service named _ipsgl_

```
show ipsg statistics name ipsgl
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ipv6

Displays the statistics for each rule in an IPv6 access control group.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show ipv6 access-group

show ipv6 { access-group [ statistics] | access-list [ list_name ] | interface [ summary | name interface_name [ statistics ] | neighbors | route route_ip_address }
```

**access-group [ statistics ]**
Displays all configured access groups in the current context along with the priority values.

*statistics:* Displays all configured access groups along with packet and byte counters for each IPv6 ACL rule hit for the current context. In addition, it shows the priority values.

**access-list [ list_name ]**
Indicates the output is to display the information for all access control lists or the list specified as `list_name`.

**interface [ summary | name interface_name [ statistics ]**
This command displays information about IPv6 interfaces. If no interface name is specified then information for IPv6 interfaces is displayed.

*summary:* Displays a summary of the interface information.

*name interface_name:* Displays information for the IPv6 interface specified. Must be followed by an `interface_name`.

*statistics:* Includes the number on inbound and outbound IP packets statistics that were registered by the kernel in the information displayed.

**neighbors**
Displays the neighbor discovery table for this context.

**route route_ip_address**
Indicates the route information to the address specified by `route_ip_address` is to be displayed. The route gateway address may be specified as needed to identify the route. `route_ip_address` using colon (`:`) separated notation.

**Usage**
Show the IPv6 information to verify and/or troubleshoot communication difficulties between to a remote host/node.
Example
The following command displays the ACL for the list named sampleACL.

    show ipv6 access-list samplev6ACL

The following command displays the interface information, including statistics, for the IPv6 interface samplev6Interface.

    show ipv6 interface samplev6Interface statistics

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show ipv6 pool

Displays information for ipv6 pools.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ipv6 pools [ name ipv6 pool name|group-name name| { grep grep_options | more } ]
```

**name ipv6 name**
Displays information for a specified ipv6 pool.

**group-name name**
Displays information for a specified IPv6 pools group.

`name` is the name of the group of IPv6 pool and must be a string having 1 to 79 alpha and/or numeric characters.

**grep grep_options | more**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to see all the ipv6 pools.

Example
The following command displays ipv6 pool information:

```
show ipv6 pools
```
show iups-service

This command displays information for Iu-PS services in the current context.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show iups-service { all | name srvc_name }{ rnc { all | mcc mcc_num mnc mnc_num | rnc_id } }

| all |
| Show information for all IuPS services. |

| name srvc_name |
| srvc_name: must be a string of 1 to 63 alphanumeric characters that identifies a specific existing IuPS service. |

| rnc all |
| Displays information for all configured RNCs. |

| rnc mcc mcc_num mnc mnc_num |
| Displays information for a specific RNC. |
| •mcc_num: The Mobile Country Code (MCC) of the RNC. Must be a 3 digit integer from 200 through 999. |
| •mnc_num: The Mobile Network Code (MNC) of the RNC. Must be a 2 or 3 digit integer from 00 through 999. |

| rnc rnc_id |
| rnc_id: The identification number of the RNC configuration instance. Must be an integer from 0 to 4095. |

Usage
Use this command to display information for a specific Iu-PS service or for all Iu-PS services configured within the context. It is also possible, but not required, to fine-tune the display to only provide information for a specific RNC.
Iu-PS services control the interface between the SGSN and the RNCs in the UMTS Radio Access Network (UTRAN). Iu-PS services include the control plane and the data plane between these nodes.

Example
The following command displays information for a single Iu-PS service named iups-svc-1:

show iups-service name iups-svc-1
The next command displays information for all Iu-PS services configured in the current context:

`show iups-service all`

This command displays information for a specific RNC for a specific Iu-PS services:

`show iups-service name iups-svc-1 rnc 123`

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show l2tp sessions

Displays information for L2TP tunnels.

Product
LNS, PDSN, GGSN, HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
full
Shows all available information for the specified sessions.

summary
Shows a summary of available information for the specified sessions.

counters
Shows counters for the specified L2TP sessions.

all
Shows all current sessions.

callid id
Show session information for the specified call id. The output of the command `show l2tp tunnels` contains a field labeled Callid Hint which lists the call id information to use with this command. This is an 8-Byte Hexadecimal number.

username name
Shows session information for the specified subscriber. `username` has a string length of 1 to 127 characters. Wildcard characters $ and * are allowed.

msid ms_id
Shows session information for the mobile user identified by `ms_id`. `ms_id` must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.

lac-service service_name
Shows all L2TP sessions in the specified LAC service.

lns-service service_name
Shows all L2TP sessions in the specified LNS service.

peer-address [ operator ] peer_address
Shows all L2TP sessions to the destination (peer LNS) at the specified IP address. The `peer_address` must be specified using the standard IPv4 dotted decimal notation.
```
In conjunction with `sessions` keyword, indicates a range of peers is to be displayed.

`peer-address [operator] peer_address` must be specified using the standard IPv4 dotted decimal notation.

`operator` implies how to logically specify a range of peer-address and it must be one of the following:

- `<`: IP address less than to specified `peer_address`
- `>=`: IP address less than or equal to specified `peer_address`
- `>=`: IP address less than to specified `peer_address`
- `less-than`: IP address less than to specified `peer_address`

### Usage

Use this command to show information for sessions in the current context.

> **Important:** If this command is executed from within the local context, cumulative session information is displayed for all contexts.

### Example

The following command displays cumulative statistics for all sessions processed within the current context:

```
show l2tp sessions
```

The following command displays all information pertaining to the L2TP session of a subscriber named `isp1vpuser1`:

```
show l2tp session full username isp1vpuser1
```

> **Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show l2tp statistics

Displays statistics for all L2TP tunnels and sessions.

Product
LNS, PDSN, GGSN, HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

lac-service service_name
Shows L2TP statistics for all tunnels and sessions in the specified LAC service.

lns-service service_name
Shows L2TP statistics for all tunnels and sessions in the specified LNS service.

peer-address peer_address
Shows L2TP statistics for all tunnels and sessions to the destination (peer LNS) at the specified IP address. The peer_address must be specified using the standard IPv4 dotted decimal notation.

Usage
Use this command to display statistics for L2TP services.

Example
The following command displays statistics for a specific LAC service named vpn1:

show l2tp statistics lac-service service_name

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show l2tp tunnels

Displays information for L2TP tunnels.

Product
LNS, PDSN, GGSN, HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>full</td>
<td>Shows all available information for the specified tunnels.</td>
</tr>
<tr>
<td>summary</td>
<td>Shows a summary of available information for the specified tunnels.</td>
</tr>
<tr>
<td>counters</td>
<td>Shows counters for the specified L2TP tunnels.</td>
</tr>
<tr>
<td>all</td>
<td>Shows all current tunnels.</td>
</tr>
<tr>
<td>callid id</td>
<td>Show tunnel information for the specified call id. The output of the command <code>show l2tp tunnels</code> contains a field labeled Callid Hint which lists the call id information to use with this command. This is an 8-Byte Hexadecimal number.</td>
</tr>
<tr>
<td>username name</td>
<td>Shows tunnel information for the specified subscriber. <code>username</code> has a string length of 1 to 127 characters. Wildcard characters $ and * are allowed.</td>
</tr>
<tr>
<td>msid ms_id</td>
<td>Shows tunnel information for the mobile user identified by <code>ms_id</code>. <code>ms_id</code> must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.</td>
</tr>
<tr>
<td>lac-service service_name</td>
<td>Shows all L2TP tunnels in the specified LAC service.</td>
</tr>
<tr>
<td>lns-service service_name</td>
<td>Shows all L2TP tunnels in the specified LNS service.</td>
</tr>
<tr>
<td>peer-address [ operator ] peer_address</td>
<td>Shows all L2TP tunnels to the destination (peer LNS) at the specified IP address. The <code>peer_address</code> must be specified using the standard IPv4 dotted decimal notation.</td>
</tr>
</tbody>
</table>
In conjunction with `tunnels` keyword, indicates a range of peers is to be displayed. `peer-address [ operator ] peer_address` must be specified using the standard IPv4 dotted decimal notation.

`operator` implies how to logically specify a range of peer-address and it must be one of the following:

- `<`: IP address less than to specified `peer_address`
- `>`: IP address less than to specified `peer_address`
- `greater-than`: IP address less than to specified `peer_address`
- `less-than`: IP address less than to specified `peer_address`

**Usage**

Use this command to show information for tunnels in the current context.

**Example**

The following command displays all of the tunnels currently being facilitated by LAC services within the current context:

```
show l2tp tunnels all
```

The following command displays information pertaining to the L2TP tunnel(s) established for a LAC-service named `vpn1`:

```
show l2tp tunnels full lac-service vpn1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show lawful-intercept

Displays information on sessions that are currently being lawfully intercepted.

Product
PDSN, HA, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, or Inspector that have l-administrator privileges.

Syntax

```
show lawful-intercept [ full ] [ all ] [ imsi imsi_value ] [ intercept-idli_id ] [ ip-addr intercept_ip_addr ] [ msid ms_id ] [ username subscriber_name ] [ statistics ]
```

<table>
<thead>
<tr>
<th><strong>full</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Display full detailed information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>all</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information for all lawful intercepts.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>imsi imsi_value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the International Mobile Subscriber Identity (IMSI) of the intercepted subscriber session.</td>
</tr>
<tr>
<td><em>imsi_value</em> is an integer value from 1 to 15 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ipaddr intercept_ip_addr</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address of the intercepted subscriber session.</td>
</tr>
<tr>
<td><em>intercept_ip_addr</em> must be specified using dotted decimal notation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>msid ms_id</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the mobile subscriber identification number of the intercepted subscriber session.</td>
</tr>
<tr>
<td><em>ms_id</em> must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>username subscriber_name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the username of the intercepted subscriber.</td>
</tr>
<tr>
<td><em>subscriber_name</em> refers to a previously configured user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>statistics</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Display summary statistical information for all Lawful Intercept sessions.</td>
</tr>
</tbody>
</table>

Usage
Use this command to display lawful intercept statistics.
Important: You must log in to the system through a Secure Shell (SSH) using a system account that has administrator privileges to use this command. For details on using the Lawful Intercept capability of the system, refer to System Administration and Configuration Guide.

Example
To show detailed information for a lawfully intercepted session with the MSID 0000100048, enter the following command

```
show lawful-intercept full msid 0000100048
```
show lac-service

Displays the information for all LAC services or for a particular LAC service.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show lac-service { all | nameservice_name } [ | { grep grep_options | more } ]

- **all**
  Display information for all LAC services.

- **name service_name**
  Display information only for the LAC service specified by `service_name`.
  `service_name` is up to a 60 character name given to the service when it was originally configured.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage
Use this command to list information for LAC services configured on this system.

Example
The following commands display information for all LAC services and the LAC service named `lac1`, respectively.

```
show lac-service all
show lac-service name lac1
```
show leds

Displays the current status of the LEDs for a specific card or all cards.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show leds { all | card_num } [ | { grep grep_options | more } ]
```

- `all` | `card_num`
  - `all`: indicates the LED status for all cards is to be displayed.
  - `card_num` indicates the LED status for the card specified by `card_num` is to be displayed.

- `grep grep_options | more`
  - Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Display the status of the LEDs as a part of an automated periodic script which checks the LEDs of the chassis.

Important: This command is not supported on all platforms.

Example
The following commands display the LED status for all cards and only card 0, respectively.

```
show leds all
```

Important: Refer to the descriptions for Card LEDs and System LEDs in `show card info` command in the Counters and Statistics Reference for information on the LED color codes.
show license information

Displays the installed license information as well as maximum number of sessions.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show licenseinformation { key_name | full } | { key } [ | { grep | grep_options } | more ]
```

- **key_name / full**
  - `key_name`: the output displays the information for the key specified as `key_name`.
  - `full`: the output displays the full features and quantities without any hardware limits in place.

- **key:**
  - indicates the output is to display the installed keys in encrypted format.

- **grep grep_options | more**
  - Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Show the license information to verify the proper keys have been installed. This command is also helpful in troubleshooting user system access due to the maximum number of sessions being reached.

Example

The following displays the encrypted installed key and the information for `sampleKey` respectively.

```
show license information
```
show linecard table

Displays information on the rear-installed interface cards.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```markdown
show linecard table [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th><strong>table</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays information on all linecard slots in tabular format.</td>
</tr>
</tbody>
</table>

| **grep grep_options | more** |
|---------------------|
| Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*. |

**Usage**

Show the line card information to verify hardware inventories and installed components.

**Important:** This command is not supported on all platforms.

**Example**

```bash
show linecard table
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show lma-service

Displays statistic and counter information for Local Mobility Anchor (LMA) services on this system.

Product
P-GW

Privilege
Inspector

Syntax

show lma-service all

show lma-service name service_name

show lma-service session [ all | callid id | counters | full | ipv6-address { <address | >address | address | greater-than address [ less-than address ] | less-than address [ greater-than address ] } | summary | username name ]

show lma-service statistics [ lma-service name ] [ [ | { grep grep_options | more } ]]

all
Displays information about all configured LMA services on this system.

name service_name
Displays configuration information for a specific LMA service configured on this system.

session [ all | callid id | counters | full | ipv6-address { <address | >address | address | greater-than address [ less-than address ] | less-than address [ greater-than address ] } | summary | username name ]

Displays session information filtered by the following parameters:

- all: Displays all active LMA sessions using LMA services on the system.
- callid id: Displays available session information for the specific call identification number. id must be an eight-digit HEX number.
- counters: Displays session counters for active LMA sessions using LMA services on the system. This keyword can also be filtered by the following:
  - all
  - callid
  - ipv6-address
  - username

Refer to the keyword descriptions in this command for information regarding these filters.

full: Displays additional session information for active LMA sessions using LMA services on the system. This keyword includes the information in the output of the ‘all’ keyword plus additional information. This keyword can also be filtered by the following:

- all
show lma-service

- `callid`
- `ipv6-address`
- `username`

Refer to the keyword descriptions in this command for information regarding these filters.

**ipv6-address:**
- `<address` and `less-than address`: Displays summary information for a group of IPv6 addresses that are less than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the `greater-than` option. `address` must be specified in colon separated notation.
- `>address` and `greater-than address`: Displays summary information for a group of IPv6 addresses that are greater than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the `less-than` option. `address` must be specified in colon separated notation.
- `address`: Displays summary information for a specific IPv6 address using an LMA service on this system. `address` must be specified in colon separated notation.

**summary** Displays the number of LMA sessions currently active for LMA services configured on the system.

**username name**: Displays available session information for a specific user in a service session. `name` must be followed by an existing user name and must be from 1 to 127 alpha and/or numeric characters.

**statistics [ lma-service name ]**

`lma-service name`: Displays LMA service statistics for a specific LMA service. `name` must be an existing LMA service and be from 1 to 63 alpha and/or numeric characters.

| { grep grep_options | more }

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of Chapter 1 of the Command Line Interface Reference Guide.

**Usage**

Use this command to view configuration information for LMA services on this system.

**Example**

The following command displays service statistics for the LMA service named `lma1`:

```
show lma-service name lma1
```
show lns-service

Displays the information for all LNS services or for a particular LNS service.

Product
PDSN, HA, GGSN, LNS

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show lns-service { all | nameservice_name } [ | { grep grep_options | more } ]
```

- **all**
  Display information for all LNS services.

- **name service_name**
  Display information only for the LNS service specified by `service_name`.
  `service_name` is up to a 60 character name given to the service when it was originally configured.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter in the `Command Line Interface Reference`.

Usage

Use this command to list information for LNS services configured on this system.

Example

The following commands display information for all LNS services and the LNS service named lns1, respectively.

```
show lns-service all
show lns-service name lns1
```
show local-user

Displays information pertaining to local-user accounts.

Product
All

Privilege
Security Administrator

Syntax

```
show local-user [ [ username name ] [ inactive filter ] [ verbose | wide ] ]
statistics [ verbose ]
```

**username name**
Specifies the name of a specific local-user administrative account for which to display information. name can be from 3 to 16 alpha and/or numeric characters in length and is case sensitive.

**inactive filter**
Specifies a filter for displaying inactive local-user accounts. filter can be one of the following:

- `< days`: Displays accounts that have been inactive less than the specified number of days.
- `>` days`: Displays accounts that have been inactive more than the specified number of days.
- `greater-than days`: Displays accounts that have been inactive more than the specified number of days.
- `less-than days`: Displays accounts that have been inactive less than the specified number of days.

days can be configured to any integer value from 1 to 365.

**[ verbose | wide ]**
Default: wide
Specifies how the information is to be displayed as one of the following options:

- `verbose` : The data is displayed in list format. Additional information is provided beyond what is displayed when the wide option is used.
- `wide` : The data is displayed in tabular format.

**statistics [ verbose ]**
Displays local-user statistics.
Using the `verbose` keyword displays additional statistics.

Usage

Use this command to display information and statistics on local-user administrative accounts.

Example

The following command displays detailed information on local-user administrative accounts that have been inactive for more than 10 days:
show local-user

**show local-user inactive greater-than 10 verbose**

The following command displays detailed information for a local-user account named Test:

**show local-user username Test verbose**

The following command displays detailed local-user account statistics:

**show local-user statistics verbose**

---

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show logging

Displays the defined logging filters for the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show logging [ active | verbose ] [ | { grep grep_options | more } ]

active | verbose
Default: all facilities are shown in concise form.
active: indicates only the active CLI logging filter information is to be displayed.
verbose: indicates the output should provide as much information as possible.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send
output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the
Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
View log filters to trouble shoot disk utilization issues.

Example
show logging
show logging active
show logging verbose
show logging active verbose
**show logs**

Displays active and inactive logs filtered by the options specified.

**Product**
- All

**Privilege**
- Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show logs [ active ] [ inactive ] [ callid call_id ] [ event-verbosistyevt_verboseness] [ facility facility ] [ level severity_level ] [ pdu-data pdu_format ] [ pdu-verbosisty pdu_verboseness ] [ procler facility ] [ since from_date_time [ until to_date_time ] ] [ | { grep grep_options | more } ]
```

**active**
Indicates output is to display data from active logs.

**inactive**
Indicates output is to display data from inactive logs.

**callid call_id**
Specifies a call ID for which log information is to be displayed. `call_id` must be specified as a 4-byte hexadecimal number.

**event-verbosisty evt_verboseness**
Specifies the level of verbosity to use in displaying of event data as one of:
- **min** - displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- **concise** - displays detailed information about the event, but does not provide the event source within the system.
- **full** - displays detailed information about event, including source information, identifying where within the system the event was generated.

**facility facility**
Specifies the facility to modify the filtering of logged information for as one of:
- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a1mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **acl-log**: Access Control List logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **all**: All facilities
- **asf**: Voice Application Server Framework logging facility
- **asfprt**: ASF Protocol Task (SIP) logging facility
- **asngwmgr**: ASN Gateway Manager facility
- **asnpemgr**: ASN Paging Controller/Location-Registry Manager facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **cli**: CLI logging facility
- **cscf**: IMS/MMD CSCF
- **cscfmgr**: SIP CSCF Manager facility
- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **dcardctrl**: IPSEC Daughtercard Controller logging facility (not used at this time)
- **dcardmgr**: IPSEC Daughtercard Manager logging facility (Not used at this time)
- **dhcp**: DHCP facility (GGSN product only)
- **dhost**: Distributed Host logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-ecs**: ECS Diameter signaling facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSEC Data Path facility
- **drvctrl**: Driver Controller facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: eGTP manager logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility (GGSN product only)
- **gtpcemgr**: GTP-C protocol Manager logging facility (GGSN product only)
- **gtp**: GTP-PRIME protocol logging facility (GGSN product only)
- **gtpu**: GTP-U protocol logging facility (GGSN product only)
• **h248prt**: H.248 Protocol logging facility
• **hamgr**: Home Agent manager logging facility
• **hat**: High Availability Task (HAT) process facility
• **ims-authoriztn**: IMS Authorization Service facility
• **ip-arp**: IP Address Resolution Protocol facility
• **ip-interface**: IP interface facility
• **ip-route**: IP route facility
• **ipsec**: IP Security logging facility
• **ipsgmgr**: IP Services Gateway facility
• **ips**: IP Pool Sharing Protocol logging facility
• **l2tp-control**: L2TP control logging facility
• **l2tp-data**: L2TP data logging facility
• **l2tpdemux**: L2TP Demux Manager logging facility
• **l2tpmgr**: L2TP Manager logging facility
• **li**: Lawful intercept facility (Logs are visible only to system accounts with li-administrator privileges.)
• **magmgr**: Mobile Access Gateway manager logging facility
• **mme-app**: Mobility Management Entity Application logging facility
• **mmedemux**: Mobility Management Entity Demux Manager logging facility
• **mme-hss**: Mobility Management Entity logging facility
• **mme-misc**: Mobility Management Entity Miscellaneous logging facility
• **mobile-ip**: Mobile IP processes
• **mobile-ip-data**: Mobile IP data facility
• **mobile-ipv6**: Mobile IPv6 logging facility
• **multicast-proxy**: Multicast Proxy logging facility
• **nas**: Network Access Signaling logging facility
• **netwstrg**: Network Storage facility
• **npctrl**: Network Processor Unit Control facility
• **npumgr**: Network Processor Unit Manager facility
• **nctrl**: Charging Service Controller facility (supported in conjunction with ECSv1)
• **nsmgr**: Charging Service Manager facility
• **nsproc**: Charging Service process facility
• **orbs**: Object Request Broker System logging facility
• **ospf**: OSPF logging facility
• **pgw**: PDN Gateway logging facility
• **ppp**: PPP link and packet facilities
• **radius-acct**: RADIUS accounting logging facility
• **radius-auth**: RADIUS authentication logging facility
show logs

- radius-coa: RADIUS change of authorization and radius disconnect
- rct: Recovery Control Task logging facility
- rdt: Redirect Task logging facility
- resmgr: Resource Manager logging facility
- rip: RIP logging facility (RIP is not supported at this time.)
- rohc: RObust Header Compression facility
- rsvp: Reservation Protocol logging facility
- sct: Shared Configuration Task logging facility
- sessctrl: Session Controller logging facility
- sessmgr: Session Manager logging facility
- st: Switch Fabric Task logging facility
- sgpw: Serving Gateway logging facility
- sipcdprt: Sip Call Distributor facility
- sitmain: System Initialization Task main logging facility
- snmp: SNMP logging facility
- srdb: Static Rating Database
- srp: Service Redundancy Protocol (SRP) logging facility
- ssh-ipsec: SSH IP Security logging facility
- stat: Statistics logging facility
- system: System logging facility
- tacacplus: TACACS+ Protocol logging facility
- threshold: threshold logging facility
- udr: User detail record facility (used with the Charging Service)
- user-data: User data logging facility
- user-l3tunnel: User layer-3 tunnel logging facility
- vpn: Virtual Private Network logging facility
- wimax-data: WiMAX DATA
- wimax-r6: WiMAX R6

```
level severity_level
```

`level severity_level` specifies the level of information to be logged, `severity_level`, from the following list which is ordered from highest to lowest:

- critical - display critical events
- error - display error events and all events with a higher severity level
- warning - display warning events and all events with a higher severity level
- unusual - display unusual events and all events with a higher severity level
- info - display info events and all events with a higher severity level
- trace - display trace events and all events with a higher severity level
show logs

- debug - display all events

**pdu-data pdu_format**
Specifies output format for the display of packet data units as one of:
- none - output is in raw format (unformatted).
- hex - output being displayed in hexadecimal format.
- hex-ascii - output being displayed in hexadecimal and ASCII similar to a main-frame dump.

**pdu-verbosity pduverbosity**
Specifies the level of verboseness to use in displaying of packet data units as a value from 1 to 5 where 5 is the most detailed.

**proclet facility**
Shows the logs from a specific proclet facility. The available facilities are the same as those listed earlier.

**since from_date_time [ until to_date_time ]**
Default: no limit.
**since from_date_time:** indicates only the log information which has been collected more recently than **from_date_time** is to be displayed.
**until to_date_time:** indicates no log information more recent than **to_date_time** is to be displayed. **until** defaults to current time when omitted.
**from_date_time** and **to_date_time** must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where YYYY is a 4-digit year, MM is a 2-digit month in the range 01 through 12, DD is a 2-digit day in the range 01 through 31, HH is a 2-digit hour in the range 00 through 23, mm is a 2-digit minute in the range 00 through 59, and ss is a 2-dig second in the range 00 through 59.
**to_date_time** must be a time which is more recent than **from_date_time**.
The use of the **until** keyword allows for a time range of log information while only using the **since** keyword will display all information up to the current time.

**grep grep_options | more**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
View log files for general maintenance or troubleshooting system issues.

**Example**
The following commands display log information for the **allmgr** facility starting with February 20th, 2003 at midnight where both are equivalent.

**show logs facility allmgr since 2003:02:20:00:00**

**show logs facility allmgr since 2003:02:20:00:00:00**

The following command displays the log information for call ID **FE881D32** only in active logs.
show logs active callid FE881D32
Chapter 95
Exec Mode Show Commands (M-P)

This section includes the commands `show m3ua statistics` through `show profile-id-qci-mapping`. 
show mag-service

Displays statistic and counter information for Mobile Access Gateway (MAG) services on this system.

Product
HSGW, S-GW

Privilege
Inspector

Syntax

```
show mag-service { all | name service_name | session [ all | callid id | counters | full | msid id | summary | username name ] | statistics [ name service_name ] } [ | { grep grep_options | more } ]
```

**all**
Displays information for all configured MAG services on this system.

**name service_name**
Displays configuration information for a specific MAG service configured on this system.

_service_name_ must be an existing MAG service, and be from 1 to 63 alpha and/or numeric characters in length.

**session [ all | callid id | counters | full | msid id | summary | username name ]**

_all:_ Displays all active MAG sessions using MAG services on the system.

_callid id:_ Displays available session information for the specific call identification number. _id_ must be an eight-digit HEX number.

_counters:_ Displays counters for all MAG services on the system. This keyword can also be filtered by the following:

- _all_
- _callid_
- _msid_
- _username_

Refer to the keyword descriptions in this command for information regarding these filters.

_full:_ Displays additional session information for all active MAG sessions using MAG services on the system. This keyword includes the information in the output of the ‘all’ keyword plus additional information. This keyword can also be filtered by the following:

- _all_
- _callid_
- _msid_
- _username_

Refer to the keyword descriptions in this command for information regarding these filters.

_msid id:_ Displays available information for a specific mobile station identification number or group of numbers based on wildcard entry. _id_ must be a valid MSID number and can be a sequence of characters.
and/or wildcard characters ('$' and/or '*'). The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (''). For example: ‘$’.

**summary** Displays the number of MAG sessions currently active for MAG services configured on the system.

**username name** Displays available session information for a specific user in a service session. *name* must be followed by an existing user name and must be from 1 to 127 alpha and/or numeric characters.

**statistics [ name service_name ]**

- **name service_name** Displays MAG service statistics for a specific MAG service. *service_name* must be an existing MAG service and be from 1 to 63 alpha and/or numeric characters.

| { grep grep_options | more } |

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of the *grep* and *more* commands, refer to the Regulating a Command’s Output section of Chapter 1 of the Command Line Interface Reference Guide.

**Usage**

Use this command to view configuration information for MAG services on this system.

**Example**

The following command displays service statistics for the MAG service named *mag1*:

```
show mag-service name mag1
```
show map-service

Displays information configured for the Mobile Application Part (MAP) services, including MAP service features and operational configuration. Also includes some related configuration information for the HLR and EIR configuration parameters.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show map-service [ all | name srvc_name ]

name srvc_name

srvc_name: must be a string of 1 to 63 alphanumeric characters that identifies a specific existing MAP service.

Usage
Use this command to display all MAP service or the statistics for a particular MAP service.

Example
The following command displays configuration information for the MAP service named map-svc-1:

    show map-service name map-svc-1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show map statistics

Displays Mobile Application Part (MAP) statistics.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show map statistics [ name svc_name ]
```

- `name svc_name`
  - `svc_name`: must be a string of 1 to 63 alphanumeric characters that identifies a specific existing MAP service.

Usage

Use this command to display all MAP statistics or the statistics for a particular MAP service.

Example

The following command displays statistics for the MAP service named `map-svc-1`:

```
show map statistics name map-svc-1
```

The following command displays combined statistics for all MAP services in the current context:

```
show map statistics
```

`Important:` Output descriptions for commands are available in the *Statistics and Counters Reference.*
show maximum-temperatures

Shows the maximum temperature reached by each card since the last temperature timestamp reset.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```plaintext
show maximum-temperatures [ verbose] [ | { grep grep_options | more } ]
```

| grep grep_options | more |
---|---|
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

| verbose |
---|
Indicates that the output is to contain detailed information.

Usage
Verify the maximum temperature reached by components in the chassis since the indicated timestamp.

**Important:** This command is not supported on all platforms.

Example

```plaintext
show maximum-temperatures
show maximum-temperatures verbose
```
show mbms bearer-service

Displays configuration information for bearer service configured for multimedia broadcast and multicast facility on this system.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show mbms bearer-service [ all | apn apn_name mcast-addr ip_address | service-type { broadcast | multicast } | full | instance instance_id | summary ] + | | { grep grep_options | more } ]
```

- **all**
  Displays information on all bearer services configured on the system.

- **apn apn_name mcast-addr ip_address**
  Displays bearer service information of MBMS for a specific APN `apn_name` bind to given BM-SC (Broadcast Multicast - Service Center) server address `ip_address`.
  `apn_name` is the name of the APN and can be from 1 to 62 alpha and/or numeric characters and is case sensitive.
  `ip_address` is the IP address of the BM-SC server in IPv4 dotted decimal notation bind to the APN.

- **service-type { broadcast | multicast }**
  Displays information for a specific type of service for MBMS.
  broadcast: Specifies the MBMS service type as broadcast only.
  multicast: Specifies the MBMS service type as multicast only.

- **full**
  Displays full information for specific or all instances of bearer service in MBMS feature on system.

- **instance instance_id**
  Displays session information filtered for specific instances of bearer service in MBMS feature on system.
  `instance_id` is the indicator for bearer service running for MBMS session and it must be an integer from 1 through 64.

- **summary**
  Displays summary information for specific or all instances of bearer service in MBMS feature on system.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more` options, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.
show mbms bearer-service

Usage

Use this command to verify the configuration of one or all bearer services and active instances of bearer services under MBMS feature. It is also useful for monitoring or troubleshooting purposes. If this command is executed from within the local context with the all keyword, information for all bearer service instances running under MBMS feature configured on the system will be displayed.

Example

The following command displays configuration information for all bearer service instances running on system:

    show mbms bearer-service full all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mipfa

Displays the foreign agent information for the mobile IP calls specified.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show mipfa { [ [ counters | full | summary ] { all | callid call_id | msid ms_id | peer-address [ operator ] peer_address | reverse-tunnel { on | off } ] | username user_name } | statistics [ fa-service fa_name | peer-address [ peer_address | greater-than peer_address | less-than peer_address | > peer_address | < peer_address ] ] | peers fa-service service_name [ current-sessions { { > | greater-than } sessions | < sessions } | { < | less-than } sessions | > sessions ] | sessions ] | peer-address address ] ) } [ [ grep grep_options | more ] ]
```

counters | full | summary

Default: concise output.
counters: indicates the output is to include the statistic counters.
full: indicates detailed information is to be displayed.
summary: indicates only summary information is to be displayed.
These options are not available in conjunction with the statistics keyword.

all | callid call_id | msid ms_id | peer-address peer_ip_address | reverse-tunnel { on | off } | username user_name

all: indicates all available information is to be displayed.
callid call_id: indicates the information only for calls with Id call_id are to be displayed.
msid ms_id: must be specified as a 4-byte hexadecimal number.
peer-address peer_ip_address: specifies a mobile subscriber ID only for which information is to be displayed. ms_id must be from 7 to 16 digits specified as an IMSI, MIN, or RMI and /or characters $ and * for wildcard filter.
reverse-tunnel { on | off }: will show any subscriber with a MSID that match the upper 8 digits of MSID supplied, i.e. 01234567 and any 2 digits at remaining 2 places.
username user_name: specifies a user only for which MIP call information is to been displayed where the user is specified as user_name.
user_name: must be a sequence of character and /or wildcard characters $ and * for wildcard matching with a string length of 1 to 127 characters.
show mipfa

```
statistics [ fa-service fa_name | peer-address [ peer_address | greater-than peer_address | less-than peer_address | > peer_address | < peer_address ]
```

Indicates the statistics information is to be displayed for foreign agent service specified as `fa_name` or for the peer specified by the address `peer_address`.

- **fa-service `fa_name`**: indicates the statistic information for the peer specified is to be displayed. `fa_name` must be from 1 to 63 alpha and/or numeric characters.
- **peer-address `peer_address`**: indicates the statistic information for the peer specified is to be displayed. `peer_address` must be specified using the standard IPv4 dotted decimal notation.
- **greater-than `peer_address`**: Specifies the range of IPv4 addresses greater than `peer_address`.
- **less-than `peer_address`**: Specifies the range of IPv4 addresses less than `peer_address`.

```
peer-address [ operator ] peer_address
```

In conjunction with `mipfa [ summary ] peer-address` keyword, indicates a range of peers is to be displayed.

- **peer-address [ operator ] peer_address**: must be specified using the standard IPv4 dotted decimal notation.
- **operator**: implies how to logically specify a range of peer-address and it must be one of the following:
  - `<`: IP address less than to specified `peer_address`
  - `>`: IP address less than to specified `peer_address`
  - `greater-than`: IP address less than to specified `peer_address`
  - `less-than`: IP address less than to specified `peer_address`

```
peers fa-service service_name [ current-sessions { ( > | greater-than ) sessions [ < sessions ] | ( < | less-than ) sessions [ > sessions ] } | sessions ] [ peer-address address ]
```

Displays peer servers for the specified FA service.

- **fa-service `service_name`**: Specifies the name of the FA service from which the associated peer servers are to be displayed. `service_name` must be an existing FA service and be from 1 to 63 alpha and/or numeric characters in length.
- **current-sessions**: Displays only peer servers with current sessions meeting the following criteria:
  - `>` or `greater-than sessions`: Displays only peer servers currently running sessions higher than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000. **Note**: the keyword “greater-than” and the “>” symbol are interchangeable in this instance of the command.
  - `< sessions`: Displays only peer servers that are currently running sessions higher than the `greater-than` parameter but less than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
  - `less-than sessions`: Displays only peer servers currently running sessions lower than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000. **Note**: the keyword “less-than” and the “<” symbol are interchangeable in this instance of the command.
  - `>` or `sessions`: Displays only peer servers that are currently running sessions lower than the `less-than` parameter but more than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
  - `sessions`: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
peer-address address: Displays only peer servers matching the IP address entered in this parameter. 
address must be specified using IPv4 dotted decimal notation and can be followed by the netmask of the address.

```
grep grep_options | more
```
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**
View MIP foreign agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

**Example**
The following displays the call information for all mobile IP FA calls and statistics for `fal`, respectively.

```
show mipfa all
```
The following command displays the statistics for the foreign agent service `fal`.

```
show mipfa statistics fa-service fal
```
The following commands displays call information for user `user0@aaa` in full detail and in summary.

```
show mipfa full username user0@aaa
show mipfa summary username user1
```
The following displays MIP FA call information for calls from mobile subscriber `4412345678` and peer address `1.2.3.4`, respectively.

```
show mipfa msid 4412345678
show mipfa peer-address 1.2.3.4
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show mipha

Displays the home agent information for the mobile IP calls specified.

Product
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show mipha [ [ counters | full | summary ] { all | callid call_id | imsi imsi_num | ip-address ip_addr | msid msid_num | peer-address [ operator ] peer_address | reverse-tunnel { on | off } | username user_name } | statistics [ ha-service ha_name | peer-address peer_address ] ] ] | peers ha-service service_name [ current-sessions { { > | greater-than } sessions { < sessions } | { < | less-than } sessions [ > sessions ] | sessions ] } ] [ { grep grep_options | more } ]
```

counters | full | summary
Default: concise output.
counters: indicates the output is to include the statistic counters.
full: indicates detailed information is to be displayed.
summary: indicates only summary information is to be displayed.
These options are not available in conjunction with the statistics keyword.

```
msid msid_num
```
Displays the subscriber with supplied MSID on HA.

msid/msid_num specifies a mobile subscriber ID only for which information is to be displayed. ms_id must be from 7 to 16 digits hexadecimal digit specified as an IMSI, MIN, or RMI and /or characters $ and * for wildcard filter.

In case of enforce imsi-min equivalence is enabled on the chasis and MIN or IMSI numbers supplied, this keyword/ filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.

```
show mipha msid ABCD0123456789 or
show mipha msid 0123456789
```
will show any subscriber with a MSID that match the lower 10 digits of MSID supplied, i.e. 0123456789.

```
show mipha msid 01234567$E
```
will show any subscriber with a MSID that match the upper 8 digits of MSID supplied, i.e. 01234567 and any 2 digits at remaining 2 places.

```
all | callid call_id | imsi imsi_num | ip-address ip_addr | msid msid_num | peer-address [ operator ] peer_address | reverse-tunnel { on | off } | username user_name
```

all: indicates all available information is to be displayed.
callid call_id: indicates the information only for calls with Id call_id are to be displayed.
call_id must be specified as a 4-byte hexadecimal number.
**imsi imsi_num** Specifies an international mobile subscriber ID only for which information is to be displayed. The IMSI (International Mobile Subscriber Identity) ID is a 15 character field which identifies the subscriber’s home country and carrier.

**ip-address ip_addr**: Show statistics for a call that has the specified IP address assigned. *ip_addr* must be an IPv4 address specified in decimal notation.

**msid msid_num** Specifies a mobile subscriber ID only for which information is to be displayed. *ms_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

**peer-address peer_address**: indicates the statistic information for the peer specified is to be displayed. *peer_address* must be specified using the standard IPv4 dotted decimal notation.

**reverse-tunnel { on | off }**: specifies either the on or off reverse IP tunnels information is to be displayed.

**username user_name**: specifies a user only for which MIP call information is to be displayed where the user is specified as *user_name*. *user_name* must be a sequence of character and/or wildcard characters $ and * for wildcard matching with a string length of 1 to 127 characters.

**peer-address [ operator ] peer_address**

In conjunction with **mipha [ summary ] peer-address** keyword, indicates a range of peers is to be displayed. *peer_address* must be specified using the standard IPv4 dotted decimal notation.

*operator* implies how to logically specify a range of peer-address and it must be one of the following:

- `<`: IP address less than to specified *peer_address*
- `>`: IP address less than to specified *peer_address*
- `*:` IP address less than to specified *peer_address*
- `less-than`: IP address less than to specified *peer_address*

**statistics [ ha-service ha_name | peer-address peer_address ]**

Indicates the statistics information is to be displayed for home agent service specified as *ha_name* or for the peer specified by the address *peer_address*.

*ha-service ha_name*: indicates the statistic information for the peer specified is to be displayed. *ha_name* must be from 1 to 63 alpha and/or numeric characters.

*peer-address peer_address*: indicates the statistic information for the peer specified is to be displayed. *peer-address peer_address* must be specified using the standard IPv4 dotted decimal notation.

**peers ha-service service_name [ current-sessions { { > | greater-than } sessions [ < sessions ] | { < | less-than } sessions [ > sessions ] | sessions ] } ] [ peer-address address ]**

Displays peer servers for the specified HA service.

*ha-service service_name*: Specifies the name of the HA service from which the associated peer servers are to be displayed. *service_name* must be an existing HA service and be from 1 to 63 alpha and/or numeric characters in length.

*current-sessions*: Displays only peer servers with current sessions meeting the following criteria:

- `>`: greater-than *sessions*: Displays only peer servers currently running sessions higher than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword “greater-than” and the “>” symbol are interchangeable in this instance of the command.
show mipha

- `< sessions`: Displays only peer servers that are currently running sessions higher than the `greater-than` parameter but less than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
- `< | less-than sessions`: Displays only peer servers currently running sessions lower than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000. **Note**: the keyword “`less-than`” and the “`<`” symbol are interchangeable in this instance of the command.
- `> sessions`: Displays only peer servers that are currently running sessions lower than the `less-than` parameter but more than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
- `sessions`: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.

peer-address `address`: Displays only peer servers matching the IP address entered in this parameter. `address` must be specified using IPv4 dotted decimal notation and can be followed by the netmask of the address.

```
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

## Usage
View MIP home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

## Example
The following displays the call information for all mobile IP HA calls and statistics for `halt`, respectively.

```
show mipha all
show mipha statistics ha-service halt
```

The following commands displays call information for user `ispluser1` in full detail and in summary.

```
show mipha full username ispluser1
show mipha summary username user1
```

The following displays MIP HA call information for calls from mobile subscribers with reverse tunneling `off` and peer address `1.2.3.4`, respectively.

```
show mipha reverse-tunnel off
show mipha peer-address 1.2.3.4
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show mipv6ha

Displays MIPv6 Home Agent-based information about selected Mobile IP calls.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show mipv6ha [ all | callid callid | counters filter | full filter | ipv6-address ip_addr | statistics mipv6ha-service mipv6ha-service_name | summary filter | username user_name ]
```

- **all**
  Displays all information for mipv6ha calls.

- **callid call_id**
  Specifies the Call Identification number.
  *call_id* must be an eight-digit HEX number.

- **counters [ all | callid | ipv6-address | username ]**
  Displays the counters associated with the HA-based MIPv6 service. The following filters are available:
  - *all*
  - *callid:
  - *ipv6-address*
  - *username*

- **full [ all | callid | ipv6-address | username ]**
  Displays all available information for the associated display or filter keyword.
  The following filters are available:
  - *all*
  - *callid:
  - *ipv6-address*
  - *username*

- **ipv6-address ip_addr**
  Displays information for subscribers connected via the packet control function with a specific or range of IP address *ipv6_address*. The address must be specified using the IPv6 colon notation.
  - *<:* Filters output so that only information less than the specified IPv6 address value is displayed.
  - *>:* Filters output so that only information greater than the specified IPv6 address value is displayed.
  - *less-than:* Filters output so that only information less than the specified IPv6 address value is displayed.
show mipv6ha

• greater-than: Filters output so that only information greater than the specified IPv6 address value is displayed.

statistics [ mipv6ha-service mipv6ha-service_name ]
Total of collected information for specific protocol since last restart or clear command.
This can be filtered according to a specified mipv6ha-service.

summary [ all | callid | ipv6-address | username ]
Displays summary information for defined sessions, based on defined parameters.
The following filters are available:
  • all
  • callid:
  • ipv6-address
  • username

username user_name
Displays session information for a specific username.

Usage
View MIPv6 home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

Example
The following displays the call information for all mobile IP HA calls and statistics for ha1, respectively.

  show mipv6ha all
The following command displays call information for user mipv6hauser1 in full detail and in summary.

  show mipv6ha full username mipv6hauser1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mme-hss service

Displays configuration and setup information of MME-HSS service(s) running on a peer or local system.

Product
MME

Privilege
Inspector

Syntax

show mme-hss service { all | name svc_name } [verbose] [{grep grep_options | more}]

| all |
| Displays configuration/setup information for all MME-HSS services configured on this system.

| name service_name |
| Displays configuration/setup information for a specific MME-HSS service configured on this system. service_name must be an existing MME-HSS service, and be from 1 to 63 alpha and/or numeric characters in length.

| verbose |
| This keyword displays the comprehensive information of specific or set of arguments. |

| { grep grep_options | more } |
| Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. |

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in CLI Overview chapter of the Command Line Interface Reference.

Usage
Use this command to view configuration/setup information for MME-HSS services on this system. This command also displays the configured actions for failure handling on various types of messages.

Example
The following command displays service statistics for all MME-HSS services configured on the system:

show mme-hss service all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mme-hss session

Displays session information of MME-HSS service(s) running on a peer or local system.

**Product**
MME

**Privilege**
Inspector

**Syntax**

```
show mme-hss session [summary | full] [all | call-id call_identifier | mdn mdn_string | nai nai_string] [verbose] [{grep grep_options | more}]
```

**summary**
This keyword displays the summarized output of this command.

**full**
This keyword displays detailed output of this command.

**all**
This keyword displays information of all MME-HSS sessions running on this system.

**call-id call_identifier**
Displays summarized or detailed statistics of MME-HSS sessions running and filtered on the basis of the call identifier with an MME-HSS service configured on this system.
`call_identifier` must an existing call identity in eight character Hex digit format running on an MME service on system.

**mdn mdn_string**
Displays summarized or detailed statistics of MME-HSS sessions running and filtered on the basis of mobile directory Number (MDN) with an MME-HSS service configured on this system.
`mdn_string` must be an alpha and/or numeric string of 1 to100 characters in length.

**nai nai_string**
Displays summarized or detailed statistics of MME-HSS sessions running and filtered on the basis of Network Access Identifier (NAI) with an MME service configured on this system.
`nai_string` must be an alpha and/or numeric string of 1 to128 characters in length.

**verbose**
This keyword displays the comprehensive information of specific or set of arguments.

```
| {grep grep_options | more}
```

This argument searches the output of the root command and selects the lines matching one or more patterns/options. The types of patterns are controlled by the options specified with `grep_options`. 
For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in CLI Overview chapter of the Command Line Interface Reference.

### Usage

Use this command to view detailed or summarized session statistics of MME-HSS sessions running on MME-HSS services on a system. This command also provides the various filter criteria to display the session statistics.

### Example

The following command displays information of all MME-HSS sessions of MME-HSS services running on a system:

```
show mme-hss session all
```

> **Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.

The following command displays summarized session information of all MME-HSS sessions running on a system:

```
show mme-hss session summary all
```

> **Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show mme-service

Displays configuration information for Mobility Management Entity (MME) services on this system.

**Product**
MME

**Privilege**
Inspector

**Syntax**

```
show mme-service { all | name svc_name } [verbose] [ | { grep grep_options | more }]
```

- **all**
  Displays configuration information for all MME services configured on this system.

- **name service_name**
  Displays configuration information for a specific MME service configured on this system.
  `service_name` must be an existing MME service, and be from 1 to 63 alpha and/or numeric characters in length.

- **verbose**
  This keyword displays the comprehensive information of specific or set of arguments.

  ```
  | { grep grep_options | more }
  ```

  Indicates the output of the command is to be piped (sent) to the command specified.
  A command to send output to must be specified.
  For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in CLI Overview chapter of the Command Line Interface Reference.

**Usage**

Use this command to view configuration information for MME services on this system.

**Example**

The following command displays service statistics for the MME service named `mme1`:

```
show mme-service name mme1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show mme-service db statistics

This command displays the MME database statistics for MME sessions for all or specific session instances on this system.

Product
MME

Privilege
Inspector

Syntax

show mme-service db statistics [instance smgr_instance] [verbose] [grep grep_options | more]

instance smgr_instance
This keyword specifies that MME database statistics are to be displayed for a specific instance of session manager running for MME service. smgr_instance must be specified as an instance ID in the range 0 through 4294967295. If instance is not specified summary statistics are displayed.

verbose
This keyword displays the comprehensive information of specific or set of arguments.

| grep grep_options | more
This argument searches the output of the root command and selects the lines matching one or more patterns/options. The types of patterns are controlled by the options specified with grep_options. For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in CLI Overview chapter of the Command Line Interface Reference.

Usage

Use this command to view database statistics for all or a particular instance of session manager for MME services on this system.

Example

The following command displays the summary database statistics for the MME service on a system:
show mme-service db statistics

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mme-service db record

This command displays the MME database records of MME sessions grouped in session instances on this system filtered with IMSI or GUTI as criteria.

Product
MME

Privilege
Inspector

Syntax

```
show mme-service db record \{all | imsi imsi_identifier | callid call_id | guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value\} [verbose] \{|grep grep_options | more\}
```

all
This keyword specifies the criteria to display all database records of a session instance used for MME service.

imsi imsi_identifier
This keyword specifies the filter criteria as International Mobile Subscriber Identity (IMSI) imsi_identifier to display the database records of a session instance. imsi_identifier is a 15 character IMSI field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘‘). For example; ‘$’.

callid call_id
This keyword specifies the filter criteria as call id call_id to display the database records of a session instance. call_id must be specified as an 8-byte hexadecimal number.

guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value
This set of keyword specifies the filter criteria as Globally Unique Temporary Identifier (GUTI) to display the database records for an MME service. The GUTI is constructed from the GUMMEI and the M-TMSI where GUMMEI is constructed from PLMN (MMC and MNC) plmn_id and MME Identifier is constructed from an MME Group ID (MMEGI) mme_grp_id and an MME Code (MMEC) mme_code. Within the MME, the mobile is identified by the M-TMSI mtmsi_value. A GUTI has; 1) unique identity for MME which allocated the GUTI; and 2) the unique identity of the UE within the MME that allocated the GUTI. Within the MME, the mobile is identified by the M-TMSI. The Globally Unique MME Identifier (GUMMEI) is constructed from public land mobile network id (PLMN) which constructed with MCC and MNC. The MME Identifier (MMEI) is constructed from an MME Group ID (MMEGI) and an MME Code (MMEC). In other words, The GUTI is constructed from the GUMMEI and the M-TMSI.

verbose
This keyword displays the comprehensive information of specific or set of arguments.
show mme-service db record

| {grep grep_options | more}

This argument searches the output of the root command and selects the lines matching one or more patterns/options. The types of patterns are controlled by the options specified with grep_options. For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in CLI Overview chapter of the Command Line Interface Reference.

Usage

Use this command to view database records for all or a particular instance of session manager for MME services on this system with IMSI or GUTI as a filter criteria.

Example

The following command displays the summary database records of a session instance for subscriber having IMSI as 123455432112345 in the MME service:

show mme-service db record imsi 123455432112345

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mme-service enodeb-association

Displays configuration information of associated eNodeB with an MME services on system.

Product
MME

Privilege
Inspector

Syntax

show mme-service enodeb-association [summary | full ] [all | mme-service-name mme_svc_name | peer-address peer_ip_address | peer-id peer_identifier] [verbose] [{grep grep_options | more }]

summary
This keyword displays the summarized output of this command.

full
This keyword displays detailed output of this command.

all
This keyword displays information of all eNodeBs associated with MME services on this system.

mme-service-name mme_svc_name
Displays summarized or detailed configuration information of eNodeBs associated with specific MME service mme_svc_name configured on this system.
mme_svc_name must be an existing MME service on system.

peer-address peer_ip_address
Displays summarized or detailed configuration information of eNodeBs associated with specific MME peer address peer_ip_address configured with an MME service on this system.
peer_ip_address must be a configured peer MME IP address in IPv4/IPv6 notation with an existing MME service on system.

peer-id peer_identifier
Displays summarized or detailed configuration information of eNodeBs associated with specific MME peer id peer_identifier configured with an MME service on this system.
peer_identifier must be a configured peer MME Id between 1 through 4294967295 with an existing MME service on system.

verbose
This keyword displays the comprehensive information of specific or set of arguments.
show mme-service enodeb-association

Usage

Use this command to view configuration information of eNodeBs associated with an MME services on this system.

Example

The following command displays detailed service statistics of associated eNodeBs with MME service named mme1:

```
show mme-service enodeb-association full mme-service-name mme1
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mme-service session

Displays session information of MME service(s) running on a peer or local system.

**Product**
MME

**Privilege**
Inspector

**Syntax**

```
show mme-service session [summary | full | counters] [all | s1-peer s1_peer_ip_address | s11-peer s11_peer_ip_address | call-id call_identifier | pdn-address pdn_ip_address] [verbose] [{grep grep_options | more}]
```

**summary**
This keyword displays the summarized output of this command.

**full**
This keyword displays detailed output of this command.

**counters**
This keyword displays all counters related events and messages for an MME session running on a system.

**all**
This keyword displays information of all MME sessions running on this system.

**s1-peer s1_peer_ip_address**
Displays summarized or detailed configuration information of MME session running and filtered on the basis of IP address of a peer connected through S1 interface with an MME service configured on this system. `s1_peer_ip_address` must be a configured IP address of a peer on S1 interface in IPv4/IPv6 notation with an existing MME service on system.

**s11-peer s11_peer_ip_address**
Displays summarized or detailed configuration information of MME session running and filtered on the basis of IP address of a peer connected through S11 interface with an MME service configured on this system. `s11_peer_ip_address` must be a configured IP address of a peer on S11 interface in IPv4/IPv6 notation with an existing MME service on system.

**call-id call_identifier**
Displays summarized or detailed configuration information of MME session running and filtered on the basis of the identifier of MME calls with an MME service configured on this system. `call_identifier` must an existing call identity in eight character Hex digit format running on an MME service on system.
**pdn-address pdn_ip_address**
Displays summarized or detailed configuration information of MME session running and filtered on the basis of IP address of connected PDN(s) with an MME service configured on this system.

*s11_peer_ip_address* must be a configured IP address of a peer on S11 interface in IPv4/IPv6 notation with an existing MME service on system.

**verbose**
This keyword displays the comprehensive information of specific or set of arguments.

| {grep grep_options | more} |
This argument searches the output of the root command and selects the lines matching one or more patterns/options. The types of patterns are controlled by the options specified with *grep_options*.
For details on the usage of the *grep* and *more* commands, refer to the Regulating a Command’s Output section in CLI Overview chapter of the Command Line Interface Reference.

**Usage**
Use this command to view session information of MME session in an MME services on this system.

**Example**
The following command displays detailed session statistics of an MME service running on a system:

```bash
show mme-service session full
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.

The following command displays detailed session counters of an MME service running on a system:

```
show mme-service session counters
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

```
show mme-service statistics

This command displays the service statistics of an MME service specified by various criteria.

Product
All

Privilege
Security Administrator, Administrator

Syntax

show mme-service statistics [sctp [mme-service mme_svc_name] | slap [mme-service mme_svc_name peer-id peer_identifier] | [emm-only | esm-only] [mme-service mme_svc_name peer-id peer_identifier] [verbose] [] | {grep grep_options | more}]

emm-only
This keyword sets the filter criteria as MME service name or peer MME identifier to display all EPS mobility management (EMM) related statistics.

esm-only
This keyword sets the filter criteria as MME service name or peer MME identifier to display all EPS session management (ESM) related statistics.

slap
This keyword sets the filter criteria as MME service name of peer MME identifier to display all S1-AP statistics.

sctp
This keyword sets the filter criteria as MME service name of peer MME identifier to display all SCTP statistics.

mme-service mme_svc_name
This keyword sets the filter criteria as MME service name to display all type of statistics of an MME service; i.e. EMM, ESM, SCTP, S1-AP, and SCTP.

peer-id peer_identifier
This keyword sets the filter criteria as identifier of MME peer to display all service statistics of an MME service; i.e. EMM, ESM, SCTP, S1-AP, and SCTP.

verbose
This keyword displays the comprehensive information of specific or set of arguments.

| { grep grep_options | more }
Indicates the output of the command is to be piped (sent) to the command specified.
A command to send output to must be specified.
For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in CLI Overview chapter of the Command Line Interface Reference.

**Usage**

This command is used to display the statistical information of an MME service based on various filter criteria as local MME service or peer MME related to EMM, ESM, SCTP, S1-AP, and SCTP.

**Example**

The following command displays the service session statistics of all MME service on a system related to all; i.e. EMM, ESM, SCTP, S1-AP, and SCTP:

```
show mme-service statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.

The following command displays the service session statistics of all MME services on a system related to S1-AP:

```
show mme-service statistics s1ap
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.

The following command displays the service session statistics of all MME services on a system related to EMM only:

```
show mme-service statistics emm-only
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show multicast-sessions

Shows information for multicast sessions defined by the specified keywords. Keywords described under Command Keywords below are base commands that display distinctive different types of data. Keywords described under Filter Keywords are filters that modify or filter the output of the base commands. Not all filter keywords are available for all command keywords commands. Each command keyword lists the filter keywords that it accepts.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show multicast-sessions [command_keyword] [filter_keywords] [ grep grep_options | more ]
```

command_keyword
The following keywords are base commands that each have a distinct display output. Only one Command Keyword can entered on the command line.

```
default
```

Displays internal call troubleshooting information for multicast sessions defined by the specified keywords.

```
callid id
```
Displays subscriber information for the call specified by id. The call ID must be specified as an 8-byte hexadecimal number.

```
flowid id
```
Displays information for a specific BCMCS flow, defined by id. The flow ID must be a hexadecimal number.

```
full
```
Displays all available multicast session information. The following filter keywords are valid for this command:

active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

```
summary
```
Only displays a summary of multicast session information. The following commands are valid for this command:

active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

filter_keywords
The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line. When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.

```
active
```
Only display information for multicast sessions that are currently active.
show multicast-sessions

**all**
If no keywords are specified before **all**, information for all multicast sessions is displayed. If keywords are specified before **all**, all information is displayed with no further options being allowed.

**callid id**
Displays multicast session information for the call specified by **id**. The call must be specified as an 8-byte hexadecimal number.

**card-num card_num**
The slot number of the processing card by which the subscriber session is processed. **card_num** is a slot number from 1 through 7 or 10 through 16.

**dormant**
Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**flowid id**
Displays information for a specific BCMCS flow, defined by **id**. The flow ID must be a hexadecimal number.

**flowid-type [ flow | program ]**
Displays information for multicast sessions according to the type of flow.

**flow**: Shows all multicast sessions for the flow ID type “**flow**”.

**program**: Shows all multicast sessions for the flow ID type “program”.

**mcast-address ipv4_address**
Show multicast sessions for a specific multicast address. Must be followed by the IP address of an interface, using dotted decimal notation.

**pcf ipv4_address**
Displays information for multicast sessions connected via the packet control function, defined by **ipv4_address**. The address must be specified using the standard IPv4 dotted decimal notation.

**pdsn-service svc_name**
Displays information for multicast session connected to the packet data service **svc_name**. The packet data service must have been previously configured.

**grep grep_options | more**
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

Please refer to the Regulating a Command’s Output of Command Line Interface Reference for details on the usage of **grep** and **more**.

**Usage**
Use this command to view information about multicast sessions.
The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant sessions.

Example
The following command displays the all broadcast-multicast sessions active in a context/system:

```
show multicast-sessions all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show network-requested-pdp-context

Displays information for the specified network-requested PDP context.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show network-requested-pdp-context imsi imsi_value
```

```
imsi imsi_value

Specifies that information will be displayed for a particular International Mobile Subscriber Identity (IMSI). imsi_value is an integer value from 1 to 15 characters.
```

Usage

Use this command to display information pertaining to network-requested PDP contexts.

Example

The following command displays network-requested PDP context information for a subscriber with an IMSI of 123456789:

```
show network-requested-pdp-context imsi 123456789
```
show network-service-entity

Displays information regarding the network service entities (NSEs) in the network.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show network-service-entity { consolidated-status | fr-config [ peer-nsei nsei] | ip-config [ nsvl { all | instance value } ] }
```

- **consolidated-status**
  Displays NSVC status information for all network service entities in the network. This keyword is particularly useful for troubleshooting.

- **fr-config [ peer-nsei nsei]**
  Displays network service configurations for NSEs using Frame Relay configurations. peer-nsei nsei including this optional keyword limits the display to a specific peer NSE identified with an integer of 0 to 65535.

- **ip-config [ nsvl { all | instance value } ]**
  Displays network service configurations for NSEs using IP configurations. Including the nsvl keyword limits the display to all or a single (instance 0 to 3) network service virtual link.

Usage
Use this command to display NSE information pertaining to the NSVCs of the NSEs in the networks or NSEs configured for Frame Relay or IP.

Example
The following command displays the status of all the NSVCs for all the NSEs in the network.

```
show network-service-entity consolidated-status
```
show nw-reachability server

Show the configuration for the network reachability servers for the current context.

Product
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show nw-reachability server { all | name server_name }
```

- **all**
  Show configuration information for all network reachability servers in the current context.

- **name server_name**
  Show configuration information for the network reachability server with the specified name.
  *server_name* is the name of a previously configured reachability server and must be a string from 1 through 15 characters in length.

Usage
Use this command to display configuration information on network reachability servers configured in the current context.

Example
The following command displays information on all network reachability servers in the current context:

```
show nw-reachability server all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ntp

Displays the network timing protocol associations and status.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ntp { associations | status } [ address ip_address ] [ | { grep grep_options | more } ]
```

**associations**
- `associations`: displays the current NTP server associations and related statistics.

**status**
- `status`: displays the client permeates configured and the synchronization status.

**address ip_address**
- `address ip_address`: the IP address of a specific NTP server/client in the current context.
  - `ip_address` must be specified using the standard IPv4 dotted decimal notation.

**grep grep_options | more**
- Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage

View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

Example

The following displays the NTP associations and status, respectively.

```
show ntp associations
show ntp status
```

**Important**: Output descriptions for commands are available in the Statistics and Counters Reference.
show orbem

Displays the ORB element manager information and statistics for the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show orbem { client { id client_name | table } | event-notif-service filters | session { id session_name | table } | status } [ | ( grep grep_options | more ) ]

**client { id client_name | table }
Indicates client information is to be displayed. The keyword table is used to output to the display information on all configured clients. The keyword id is used to specify a specific client for which information is to be displayed specified as client_name.
client_name must refer to an existing client which is found using the table keyword option.

**event-notif-service filters
Displays information pertaining to filters configured for the ORB Notification Service.

**session { id session_name | table }
Indicates session information is to be displayed. The keyword table is used to output to the display information on all configured clients. The keyword id is used to specify a specific session for which information is to be displayed specified as session_name.
session_name must refer to an existing session which is found using the table keyword option.

**status
Indicates the ORB element manage server status information is to be displayed.

**grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

**Usage
Display current sessions when ORBEM system response may appear sluggish. This command is also useful in periodic verification of the server status.

**Example
The following commands will display the information for all clients.
show orbem client table
The following commands display the information for the clientName and sessionID, respectively:

show orbem client id clientId
show orbem session id sessionId

The following command displays the ORBEM server status:

show orbem status

The following command displays the information for all sessions:

show orbem session table

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show patch-progress

This command displays the status of the on-going software patch installation.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show patch-progress
```

**Usage**
Use this command to show the status of an on-going software patch installation.

> **Important:** Software Patch Upgrades are not supported in this release.
show pdg-service

Displays configuration information about PDIF services configured on the system.

Product
PDG/TTG

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```plaintext
show pdg-service { all | name service_name }
```

- **all**
  Displays information for all configured PDG services.

- **name service_name**
  Displays information for the specified PDG service only.
  `service_name` must be the name of an existing PDG service in the current context and from 1 to 63 alpha and/or numeric characters.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage

Use this command to display information for PDG services.

Example

The following command displays available information for all active PDG services:

```plaintext
show pdg-service all
```
show pdg-service statistics

Displays statistics for the PDG/TTG since the last restart or clear command. The output includes the number of each type of protocol message. For example, the output includes the various types of EAP messages.

Product
PDG/TTG

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show pdg-service statistics [ name service_name | peer-address ipv4_address ]

name service_name
Displays statistics for the specified PDG service.

service_name must from 1 to 63 alpha and/or numeric characters.

peer-address ipv4_address
Displays statistics for a specific subscriber with the specified WLAN IPv4 address.

ipv4_address must be entered in standard IPv4 dotted decimal notation.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to display PDG service statistics.

Example
The following command displays statistics for all active PDG services:

show pdg-service statistics
**show pdif-service**

Displays configuration information about PDIF services configured on the system.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show pdif service { all [ counters ] | name name [ counters ] | statistics [ name name | peer-address address ] } [ | { grep | grep_options | more } ]
```

- **all [ counters ]**
  Displays configuration information and statistic counters for all PDIF services in the system.

- **name name [ counters ]**
  Displays configuration information and statistic counters for a specified PDIF service in the system. `name` must be from 1 to 63 alpha and/or numeric characters and an existing PDIF service.

- **statistics [ name name | peer-address address ]**
  `name name`: Displays service statistics for a specific PDIF service. `name` must be from 1 to 63 alpha and/or numeric characters and an existing PDIF service.
  `peer-address address`: Displays service statistics for a specific peer server. `address` must be specified in IP v4 dotted decimal notation.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

**Usage**
Use this command to display configuration information and statistics about PDIF services on the system.

**Example**
The following example displays configuration information about a PDIF service named `pdif23`:

```
show pdif service name pdif23
```

**Important**: Output descriptions for commands are available in the Statistics and Counters Reference.
show pdsn-service

Displays information on configured packet data services for the current context.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show pdsn-service ( all | name pdsn_name ) [ pcf-status [ address ip_address ] | filter [ all | icmp-monitored | no-calls | summary | up ] ] [ | { grep grep_options | more } ]
```

- `all | name pdsn_name`: displays information for all configured packet data services. `name pdsn_name`: indicates information only for the PDSN service specified is displayed. `pdsn_name` must be the name of an existing PDSN service in the current context and must be from 1 to 79 alpha and/or numeric characters.

- `pcf-status | address ip_address | filter [ all | icmp-monitored | no-calls | summary | up ]`: provides information on configured packet data services. `address ip_address`: only list information for the PCF with the specified IP address. `ip_address` must be specified in IP v4 dotted decimal notation. `filter`: Filter the output so only the specified information is displayed. If filter is specified with no keywords summary information for all PCFs is displayed.
  - `all`: Show information for all the PCFs
  - `icmp-monitored`: Show information only for PCFs which are ICMP monitored
  - `no-calls`: Show information only for PCFs which have no active sessions
  - `summary`: Show only a summary of the status of the PCFs
  - `up`: Show information only for PCFs which are alive

- `grep grep_options | more`: Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Show the PDSN service information for standard system monitoring or troubleshooting.

Example
The following will display the information for the sampleService and for all configured services, respectively.
show pdn-service

show pdn-service all
show pdn-service name sampleService
show pgw-service

Displays configuration information for PDN Gateway (P-GW) services on this system.

Product
P-GW

Privilege
Inspector

Syntax

```
show pgw-service { all | name service_name | statistics { all | name service_name } } [ | { grep grep_options | more } ]
```

`all`
Displays configuration information for all P-GW services configured on this system.

`name service_name`
Displays configuration information for a specific P-GW service configured on this system. `service_name` must be an existing P-GW service, and be from 1 to 63 alpha and/or numeric characters in length.

`statistics { all | name service_name }`
Displays P-GW service statistics.
`all`: Displays statistics for all P-GW services on the system.
`name service_name`: Displays statistics for a specific P-GW service. `name` must be an existing P-GW service and be from 1 to 63 alpha and/or numeric characters.

`| { grep grep_options | more }`
Indicates the output of the command is to be piped (sent) to the command specified. A command to send the output to must be specified. For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of Chapter 1 of the Command Line Interface Reference Guide.

Usage
Use this command to view configuration information for P-GW services on this system.

Example
The following command displays service statistics for the P-GW service named `pgw1`:

```
show pgw-service name pgw
```
show port

Displays information such as statistics and information on configured ports.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show port { datalink counters [ slot/port ] | info { slot/port } [ vlan vlan_id ] | npu counters [ slot/port [ tagged | untagged | vlan tag_id ] ] | table | utilization table } [ | { grep grep_options | more } ]

datalink counters slot/port

Display the information for all data links or only the one specified by slot/port. slot/port must refer to a previously configured port.

info { slot/port } [ vlan vlan_id ]

Display detailed information for all ports within the chassis or only the one specified by slot/port. slot/port must refer to a previously configured port.

vlan vlan_id: Display detailed information about all VLANs in the port/slot. If the optional vlan_id is not specified, it will show port information for all VLANs in slot/port.

npu counters [ slot/port [ tagged | untagged | vlan tag_id ] ] | bound | unbound

Display the information for network processing unit ports. The information for all ports is output or only the one specified by slot/port. slot/port must refer to a previously configured port.

tagged: Display stats for all tagged packets.
untagged: Display statistics for all untagged packets.
vlan tag_id: Display NPU counters for a specified VLAN. tag_id must be the VLAN tag ID of a previously configured VLAN.
bound: Displays individual and cumulative npu port counters for the bound ports within the current context. If the command is invoked the local context all of the bound ports for all contexts and cumulative counter values for all contexts is displayed.
unbound: Displays individual and cumulative npu port counters for all unbound ports within system.

table

Display information on all physical ports on rear-installed interface cards.

utilization table

Show average port utilization in Mbps. The output is a table that lists the current utilization average, a 5 minute average, and a 15 minute average, for all enabled ports.
show port

**grep** *grep_options | more*

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

### Usage

Display port information for troubleshooting of network communications by viewing statistics and configuration information for physical ports.

### Example

The following displays detailed information for port 1 in slot 17:

```
show port info 17/1
```

The following displays information for the data link port 33/1:

```
show port datalink counters 33/1
```

```
show port npu counters 33/1
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show power

Displays information about installed cards with power supplied.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show power [ all | chassis | card_num ] [ | { grep grep_options | more } ]
```

- **all | chassis | card_num**
  - Default: chassis
  - **all**: indicates power information for all cards is to be displayed.
  - **chassis**: indicates the chassis power source(s) are to be displayed.
  - **card_num**: specifies a specific card for which power information is to be displayed. Card number must be a value in the range 1 through 48.

- **grep grep_options | more**
  - Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  - For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
View power source information to quickly check the power for all cards within a chassis.

**Important:** On some platforms, only **show power** is supported with no other keywords or variables.

Example
The following displays power supply status for the chassis.

```
show power
```

The following command displays the power status for all slots

```
show power all
```
**show ppp**

Displays the point-to-point protocol information, detailed or summarized, for one or all connections by the use of filtering options.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show ppp { [ counters | full | summary ] { all | callid call_id | imsi id | msid ms_id | username user_name } | statistics [ pcf-address [ pcf_ip_addr | all ] | pdn-service pdn_name ] } [ | { grep grep_options | more } ]
```

- **counters | full | summary**
  
  Provides an optional modifier to the output for the level and type of information.
  
  - **counters**: indicates the point-to-point protocol statistics are to be displayed.
  
  - **full**: indicates all available information is to be displayed.
  
  - **summary**: indicates only a summary of available information is to be displayed.

- **all | callid call_id | imsi imsi_id | msid ms_id | username user_name**

  - **all**: indicates all available information is to be displayed.
  
  - **callid call_id**: indicates the PPP information only for the call specified by `call_id` is to be displayed. `call_id` must be specified as a 4-byte hexadecimal number.
  
  - **imsi id**: specifies that PPP information only for the subscriber with the specified id be displayed. The IMSI (International Mobile Subscriber Identity) `id` is a 15 character field which identifies the subscriber’s home country and carrier.
  
  - **msid ms_id**: specifies a mobile subscriber ID only for which information is to be displayed. `ms_id` must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.
  
  - **username user_name**: specifies a user only for which PPP information is to be displayed where the user is specified as `username`.

- **statistics [ pcf-address [ pcf_ip_addr | all ] | pdn-service pdn_name ]**

  Statistics for all packet data services is displayed.
  
  - **pcf-address [ pcf_ip_addr | all ]**: Display statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. `pcf_ip_addr` must be specified using the standard IPv4 dotted decimal notation.
  
  - **pdn-service pdn_name**: Display statistics only for the service specified by `pdn_name`. `pdn_name` must be from 1 to 63 alpha and/or numeric characters.

- **grep grep_options | more**

  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.
**Usage**

View the Point-to-Point Protocol information to support troubleshooting subscriber connections by viewing information for point-to-point connections for a specific subscriber.

**Example**

The following displays the PPP summary for all connections.

```
show ppp summary all
```

The following outputs the point-to-point detailed information for the user `user1`.

```
show ppp full username user1
```

The following command displays the standard information for the call with ID `FF0E11CD`.

```
show ppp callid ff0e11cd
```

The following command displays the PPP statistics for `pdsn1`.

```
show ppp statistics pdsn-service pdsn1
```

The following command provides summarized information for the PPP statistics.

```
show ppp
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show prepaid 3gpp2

This command displays prepaid accounting information for all services or only the service specified.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
all
This keyword displays prepaid statistics for all services.

ggsn-service
Display statistics for GGSN service(s).

ha-service
Display statistics for HA service(s).

lns-service
Display statistics for LNS service(s).

pdsn-service
Display statistics for PDSN service(s).

{ all | name service_name }
all: Display statistics for all services of the specified type.
name service_name: Display statistics for the service named service_name of the specified service type.

per-service-summary
Displays prepaid statistics per service summary for all services.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Displays Pre-paid statistics for a particular named service or for all services.
Example
To display statistics for a PDSN service name PDSN1, enter the following command:

```
show prepaid 3gpp2 statistics pdsn-service name PDSN1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show prepaid wimax

This command displays prepaid WiMAX accounting information for all services or only the service specified.

Product
ASN GW

Privilege
Inspector

Syntax

show prepaid wimax [ statistics { all | asngw-service { all | nameservice_name } | ha-service { all | nameservice_name } | per-service-summary } [ grepgrep_options | more ] ]

all
This keyword displays prepaid statistics for all services.

asngw-service
Displays prepaid statistics for ASN GW service(s).

ha-service
Displays prepaid accounting statistics for HA service(s).

{ all | nameservice_name }
all: Display statistics for all services of the specified type.
name service_name: Display statistics for the service named service_name of the specified service type.

per-service-summary
Displays prepaid statistics per service summary for all services.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to display prepaid WiMAX accounting statistics for named service or for all services.

Example
The following command displays prepaid WiMAX accounting statistics for an ASN GW service name asn1:

show prepaid wimax statistics asngw-service name asn1
show prepaid wimax

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show profile-id-qci-mapping

Displays QCI-RAN mapping tables configured on this system.

Product
HSGW

Privilege
Inspector

Syntax

show profile-id-qci-mapping table { all | name name } [ | { grep grep_options | more }]

- **all**
  Displays information for all QCI-RAN mapping tables configured on this system.

- **name name**
  Displays information for a QCI-RAN mapping tables configured for a specific QCI-RAN table on this system.
  *name* must be an existing QCI-RAN table, and be from 1 to 63 alpha and/or numeric characters in length.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of *grep* and *more*, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage
Use this command to display the contents of a specific QCI-RAN mapping table or all mapping tables configured on this system.

Example
The following command displays the contents of a QCI-RAN mapping table named *table1*:

```bash
show profile-id-qci-mapping table name table1
```
Chapter 96
Exec Mode Show Commands (Q-S)

This section includes the commands qci-qos-mapping through show system uptime.
show qci-qos-mapping

Displays QCI-QoS mapping tables configured on this system.

**Product**
HSGW, P-GW, S-GW

**Privilege**
Inspector

**Syntax**

```
show qci-qos-mapping table { all | name table_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all QCI-QoS mapping tables configured on this system.

- **name table_name**
  Displays information for a QCI-QoS mapping tables configured for a specific QCI-QoS table on this system. `table_name` must be an existing QCI-QoS table, and be from 1 to 63 alpha and/or numeric characters in length.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the Command Line Interface Reference.

**Usage**

Use this command to display the contents of a specific QCI-QoS mapping table or all mapping tables configured on this system.

**Example**

The following command displays the contents of a QCI-QoS mapping table named `table1`:

```
show qci-qos-mapping table name table1
```
show qos npu inter-subscriber traffic

Displays configuration information pertaining to NPU QoS priority queue bandwidth allocation and sharing.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show inter-subscriber traffic { bandwidth | bandwidth-sharing }
```

- **bandwidth**
  Displays NPU QoS priority queue bandwidth allocation configuration information.

- **bandwidth-sharing**
  Displays NPU QoS priority queue bandwidth sharing configuration information.

Usage

Use this command to verify configuration information and for troubleshooting.
When the bandwidth keyword is used, the output is a table showing the configuration status, the priority queue, and the bandwidth allocation per DSCP.
When the bandwidth-sharing keyword is used, the output of is a table displaying the bandwidth sharing configuration per processing card slot/CP number.
For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

**Important:** This functionality is not supported for use with the PDSN at this time.
show qos npu stats

Displays NPU Qos statistics per priority queue for a particular processing card:

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show qos npu stats inter-subscriber traffic slot slot_num
```

```
slot slot_num
```

Specifies the chassis slot number in which the processing card for which to display statistics is installed. `slot_num` is an integer from 1 to 48 that represents the slot in which a processing card is installed. Processing cards can be installed in slots 1 through 8, and/or 10 through 16.

Usage

This command displays packet and byte counts per NPU QoS priority queue on a per-processing card basis. For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

**Important:** This functionality is not supported for use with the PDSN at this time.

Example

The following command displays NPU QoS priority queue statistics for a processing card installed in chassis slot number 4:

```
show qos npu stats inter-subscriber traffic slot 4
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show radius

Displays and statistic information for accounting and/or authentication.

Product
PDSN, HA, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show radius { accounting servers | authentication servers } [ detail ] [ admin-status { enabled | disabled } | [ | { grep grep_options | more } ] [ radius group group_name{ detail } | [ | { grep grep_options | more } ] ] ]
```

- **accounting servers**
  Lists information for configured accounting servers and their current state.

- **authentication servers**
  Lists information for configured authentication servers and their current state.

- **[ detail ]**
  Displays historical state information for configured servers of the specified type

- **admin-status { enabled | disabled }**
  Displays information for accounting and/or authentication servers with an administrative status of “enabled” or “disabled”.

- **radius group group_name**
  Displays the authentication/authorization RADIUS server group information for server group `group_name` with in current context.
  `group_name` will be a string of size 1 to 63 character and specifies the name of server group configured in specific context for authentication/accounting.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Display the RADIUS server information as part of periodic monitoring of the health of the system.

Example

The following displays the information on configured accounting servers:
**show radius accounting server**

The following command displays detailed information for RADIUS accounting servers:

```
show radius accounting servers detail
```

The following command displays detailed information for RADIUS server group `star1` used for authentication:

```
show radius authentication servers radius group star1 detail
```

The following command displays detailed information for RADIUS server group `star1` used for accounting:

```
show radius accounting servers radius group star1 detail
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show radius charging servers

This command displays the RADIUS authentication and accounting servers or server group that are configured for use by charging services.

Product
PDSN, HA, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax
show radius charging servers [ radius group group_name ] [ | { grep grep_options | more } ]

radius group group_name all
Displays all RADIUS counter information for the specified server group configured for use by charging services.
group_name specifies the name of server group configured in specific context for authentication/accounting, and must be a string of 1 through 63 characters in length.

grep grep_options | more
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to display information about RADIUS servers or server group configured for use by Charging Services.

Example
The following command displays RADIUS servers configured for Charging Services:

show radius charging servers

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show radius client

Displays information about the RADIUS client configured on the system.

Product
PDSN, HA, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show radius client status [ | { grep grep_options | more } ]

status
Displays a status summary for the RADIUS client.

| { grep grep_options | more } |
Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
The configuration of the RADIUS protocol on the system enables RADIUS client functionality.
This command is used to view information pertaining to the status of the client.

Example
The following command displays detailed information pertaining to the system’s RADIUS client:

show radius client status

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show radius counters

Displays RADIUS server and statistic information for accounting and/or authentication.

Product
PDSN, HA, GGSN, ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show radius counters { all | radius group group_name [all] | server ip_address [port number] | summary [ all-contexts [ verbose ] ] } [ | { grep grep_options | more } ]
```

counters { all | server ip_address [ port number ] }

counters { all | server ip_address [port number] }: indicates the statistics for either all servers or the server specified by ip_address is to be displayed. The statistics for a specific port of the server may also be specified as number. ip_address must be specified using the standard IPv4 dotted decimal notation. number must be a value from 0 through 65535.

radius group group_name all

Displays all RADIUS counter information for the specified server group within current context. group_name specifies name of the server group configured in specific context for authentication/accounting, and must be a string of 1 through 63 characters in length.

summary [ all-contexts [verbose]]

Displays a summary of RADIUS statistics for all the RADIUS servers configured in specific context. all-contexts: Specifies that a summary of RADIUS statistics for all RADIUS servers configured in all contexts should be displayed. If verbose is also specified the information is displayed in more detail.

grep grep_options | more

Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Display the RADIUS server information as part of periodic monitoring of the health of the system.

Example

The following command displays detailed information pertaining to the RADIUS server group star1 with in current context:

```
show radius counters radius group star1 all
```
The following displays the statistics for the server with IP address 1.2.3.4, then just port 7777, followed by all services.

```
show radius counters server 1.2.3.4
show radius counters server 1.2.3.4 port 7777
show radius counters all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show resources

Displays the resource information by CPU or session.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```plaintext
show resources { cpu | session } [ | { grep grep_options | more } ]
```

cpu | session
--- | ---
cpu: indicates the resource information is to be displayed by CPU.
session: indicates the resource information is to be displayed by session.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

View resource utilization as part of troubleshooting systems which appear sluggish or are having excessive connection timeouts or other connection issues.

Example

The following display the resource information by CPU and session, respectively.

```plaintext
show resources cpu
show resources session
```

`Important:` Output descriptions for commands are available in the Statistics and Counters Reference.
**show rohc counters**

This command displays ROHC counters for all active calls.

**Product**

PDSN, HSGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show rohc counters [ all | callid call_id | imsi imsi_num | ip-address ip_addr | msid msid_num | username user_name ] [ | { grep grep_options | more } ]
```

- **all**
  
  Indicates all information is to be displayed.

- **callid call_id**
  
  `call_id` indicates the information only for calls with ID `call_id` are to be displayed. `call_id` must be specified as a 4-byte hexadecimal number.

- **imsi imsi_num**
  
  `imsi_num` specifies an international mobile subscriber ID only for which information is to be displayed. The IMSI (International Mobile Subscriber Identity) ID is a 15 character field which identifies the subscriber’s home country and carrier.

- **ip-address ip_addr**
  
  `ip_addr` specifies a mobile subscriber IP address only for which information is to be displayed. `ip_addr` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **msid msid_num**
  
  `msid_num` specifies a mobile subscriber ID only for which information is to be displayed. `msid_num` must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

- **username user_name**
  
  `user_name` specifies a user only for which R-P information is to be displayed where the user is specified as `user_name`.

- **grep grep_options | more**
  
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output must be specified.
  
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

---

Cisco ASR 5000 Series Command Line Interface Reference

2478

OL-22948-01
Use this command to display ROHC counters for all active calls.

Example
The following command displays ROHC counters for all active calls:

    show rohc counters all
show rohc statistics

This command displays statistics and counters for ROHC IP header compression.

**Product**
PDSN, HSGW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show rohc statistics [ psdn-service pdsnsvc_name | hsgw-service hsgwsvc_name ] [ ( grep grep_options | more ) ]
```

- **psdn-service pdsnsvc_name**
  Display ROHC statistics and counters for the specified PDSN service.

- **hsgw-service hsgwsvc_name**
  Display ROHC statistics and counters for the specified HSGW service.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to display ROHC statistics for all services or for a specific PDSN or HSGW.

**Example**

The following command displays ROHC statistics for the PDSN service named psdn1:

```
show rohc statistics psdn-service psdn1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
**show route-map**

This command displays entries for all route maps for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show route-map [ name route-map name | { grep grep_options | more } ]
```

- **name route-map name**
  Displays information for a specified route-map. The name is a string of 1 to 79 characters.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to see the rules configured in all route-maps for the current context.

**Example**

The following command displays the route-map information;

```
show route-map
```

Refer to the match and set command descriptions in Route-map Configuration Mode Commands for explanations of the various entries listed.
show rp

Displays the R-P interface statistics using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show rp [ counters | full | summary ] { all | callid call_id | msid ms_id | peer-address peer_ip_address | username user_name } [ | { grep grep_options | more } ]

counters | full | summary
Provides an optional modifier to the output for the level and type of information. counters: indicates the R-P protocol statistics are to be displayed. full: indicates all available information is to be displayed. summary: indicates only a summary of available information is to be displayed. These options are not available in conjunction with the keywords statistics or service-option statistics.

all | callid call_id | msid ms_id | peer-address peer_ip_address | username user_name

all: indicates all R-P information is to be displayed. callid call_id: indicates the information only for calls with Id call_id are to be displayed. call_id must be specified as a 4-byte hexadecimal number. msid ms_id: specifies a mobile subscriber ID only for which information is to be displayed. ms_id must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. peer-address peer_ip_address: specifies the peer IP address, of the PCF, for which R-P information is to be displayed. peer_ip_address must be specified using the standard IPv4 dotted decimal notation. username user_name: specifies a user only for which R-P information is to be displayed where the user is specified as user_name.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
View the R-P interface statistics for the current context.

Example
The following displays the summary for all connections.
show rp summary all
The following outputs the R-P interface detailed information for the user user1.

show rp full username ispluser1
The following command displays the standard information for the call with ID FF0E11CD

show rp callid ff0e11cd
The following displays the statistics summary for the R-P facility.

show rp

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show rp service-option

Displays the R-P service option statistics using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show rp service-option statistics number svc_option_num | pdsn-service pdsn_name ] [ | { grep grep_options | more } ]
```

- `number svc_option_num | pdsn-service pdsn_name`
  Default: display statistics for all service options numbers and associated packet data services.
  - `number svc_option_num` specifies the service option number for which collected statistics are to be displayed.
  - `pdn-service pdsn_name`: specifies the packet data service for which the collected statistics are to be displayed.

- `grep grep_options | more`
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
View the R-P service option statistics for the current context.

Example
The following displays the statistics for all service options.

```
show rp service-option statistics
```

The following displays the statistics for service option 5.

```
show rp service-option statistics number 5
```

The following command displays the statistics for all service options in collected for the packet data service `sampleService`.

```
show rp service-option statistics pdsn-service sampleService
```
show rp statistics

Displays the R-P protocol statistics using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show rp statistics [ pdsn-service pdsn_name | peer-address [peer_address | all]] [ | grep grep_options | more ] [ verbose ]

pdsn-service pdsn_name | peer-address peer_address

Default: all R-P protocol statistics are to be displayed.

pdsn-service pdsn_name: indicates the statistic information for the service specified is to be displayed. pdsn_name must be from 1 to 63 alpha and/or numeric characters.

peer-address [ peer_address | all]: indicates the statistic information for the peer specified or all peers is to be displayed. peer_address must be specified using the standard IPv4 dotted decimal notation.

grep grep_options | more

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

verbose

Displays more detailed statistics.

Usage

View the R-P statistics for the current context.

Example

The following displays all collected R-P statistics.

show rp statistics

The following displays the R-P statistics associated with the peer address 1.2.3.4.

show rp statistics peer-address 1.2.3.4

The following command displays the R-P statistics for the packet data service PCFnet.

show rp statistics pdsn-service PCFnet
show rp statistics

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show rsvp counters

Displays the rsvp counters using the filtering options specified.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show rsvp counters [ all | callid call_id | msid ms_id | username user_name ]
```

- **all**: indicates all rsvp information is to be displayed.
- **callid call_id**: indicates the information only for calls with Id `call_id` are to be displayed.
- **msid ms_id**: specifies a mobile subscriber ID only for which information is to be displayed. `ms_id` must be specified as a 4-byte hexadecimal number.
- **username user_name**: specifies a user only for which rsvp information is to be displayed where the user is specified as `user_name`.

**Usage**

View the rsvp counters for the current context.

**Example**

The following displays all collected rsvp counters.

```
show rsvp counters all
```
show rsvp statistics

Displays the rsvp statistics using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show rsvpcounters [ pdsn-service service | sessmgr instance instance ]
```

```
pdsn-service service | sessmgr instance instance

pdsn-service service: indicates the statistic information for the service specified is to be displayed. pdsn_name must be from 1 to 63 alpha and/or numeric characters.

sessmgr instance instance: indicates the session manager instances.
```

Usage
View the rsvp statistics for the current context.

Example
The following displays collected rsvp statistics for a sampleService.

```
show rsvp statistics pdsn-service sampleService
```
show sccp-network

This command displays SS7 Signaling Connection Control Part (SCCP) network configuration and status information.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show sccp-network { ntwk_index | all } [ status [ all | dpc ] ]
```

- **ntwk_index**
  Display configuration and status information for the SSCP network configuration with the specified network index.
  `ntwk_index` must be an integer from 1 through 12.

- **all**
  Display all available configuration and status information for all SSCP networks.

- **status all**
  Display all status information for specified SCCP networks.

- **status dpc**
  Display status information for the device in the SCCP network identified by the destination point-code.

**Usage**
Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or network.

**Example**
The following command displays global SCCP statistics:

```
show sccp-network all
```

The following command displays information for an SCCP network configuration with the network index of 1:

```
show sccp-network 1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show sccp statistics

This command displays SS7 Signaling Connection Control Part (SCCP) statistics for services that use the SCCP protocol.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show sccp statistics [ iups-service iups_srvc_name | map-service map_srvc_name | sccp-network ntwk_index ]
```

### iups-service iups_srvc_name
Display SCCP protocol statistics for the specified IU-PS service in the current context. `iups_name` must be the name of a configured IU-PS service and must be an alphanumeric string of from 1 through 63 characters.

### map-service map_srvc_name
Display SCCP protocol statistics for the specified MAP service in the current context. `map_srvc_name` must be the name of a configured MAP service and must be an alphanumeric string of from 1 through 63 characters.

### sccp-network ntwk_index
Display SCCP protocol statistics for the SSCP network configuration with the specified network index. `ntwk_index` must be an integer from 1 through 12.

**Usage**
Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or network.

**Example**
The following command displays global SCCP statistics:

```
show sccp statistics
```

The following command displays SCCP statistics for the IuPS service named `iups-serv1`:

```
show sccp statistics iups-service iups-serv1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show session counters historical

Displays historical information for session-related counters based on data collected in bulk statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show session counters historical { all | arrived | callops | connected | disconnected | failed | handoff | rejected | renewal } [ all-intervals | recent-intervals ] [ cumulative | incremental ] [ graph | table ]

---

all
Displays data for all counters either as a single, wide table or as multiple graphs.

arrived
Displays only data for “total calls arrived” counters. This is based on the “sess-ttlarrived” statistic in the system schema.

callops
Displays data for all call operations. This is a calculated value based on the following formula:
(arrived + rejected + disconnected + failed + handoffs + renewals)

connected
Displays only data for “total calls connected” counters. This is based on the “sess-ttlconnected” statistic in the system schema.

disconnected
Displays only data for “total calls disconnected” counters. This is based on the “sess-ttldisconnect” statistic in the system schema.

failed
Displays only data for “total calls failed” counters. This is based on the “sess-ttlfailed” statistic in the system schema.

handoff
Displays only data for “total handoffs” counters. This is based on the “sess-ttlhandoff” statistic in the system schema.

rejected
Displays only data for “total calls rejected” counters. This is based on the “sess-ttlrejected” statistic in the system schema.
### show session counters historical

**renewal**
Displays only data for “total renewal” counters. This is based on the “sess-ttlrenewal” statistic in the system schema.

**all-intervals**
Displays all available historical information from all samples. This filter is used by default.

**recent-intervals**
Displays historical information for only recent samples.

**cumulative**
Displays total data for all samples up to and including the last one. In this view, values increase over time.

**incremental**
Displays data changes for each specific sample. The data for each sample is the amount of change since the previous sample. This filter is used by default.

**graph**
Displays data in graphical form.

**table**
Displays data in tabular form. This is the default view.

### Usage
This command provides the ability to track key session-related statistic information over time. This information can be used as part of system performance monitoring and capacity planning.

**Important:** The information provided in the output of this command requires that bulk statistics functionality be enabled on the system. Refer to the System Administration and Configuration Guide for more information on configuring/enabling bulk statistics support.

The output of this command displays historical data collected at various sample intervals. The interval length is 15 minutes and is not user-configurable. Up to 192 samples (2 days worth of data) are maintained.

**Important:** Data collection is “best-effort” over these intervals. Data is preserved on system management card switchovers. As with all counters, certain session failures can cause inaccuracies with counters, including counters which appear to go backwards.

Each sample is identified by a timestamp that displays the approximate time the data was gathered. It is in the format YYYY:MM:DD:HH:MM:SS.

Data acquired during the sample may be marked with an “S” appended to the end of the timestamp or to the counter value. The “S” indicates that the data is suspect (potentially bad). Occurrences of this result from events like changes to the real time clock, which can cause an interval to be an atypical length. Instances of suspect data should be rare. Additionally, there may be occasions in which a sample may be marked as
“invalid”. “invalid” identifies bad data, a situation that could result from the polling hasn't run long enough, or because of an unexpected error retrieving data. Since baseline values must be obtained prior to collecting interval samples, the first interval of data will not be available until up to 2x the interval period.

**Example**
The following command displays cumulative total calls arrived information for the most recent intervals and displays the output in graphical format:

```
show session counters historical arrived recent-intervals cumulative graph
```

The following command displays historical data for all counters for all intervals and displays the output in tabular format:

```
show session counters historical all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show session counters pcf-summary

Displays the PCF summary which include the number of calls, call types, and Tx/Rx packets/octet statistics.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show session counters pcf-summary [ call-types | data | wfl [ pcf pcf_address ] [ | { grep grep_options | more } | ] ]
```

- **call-types**
  Displays the number of calls and the types of calls.

- **data**
  Displays the number of successful calls and Tx/Rx packets/octet statistics.

- **pcf pcf_address**
  Displays the given PCF summary for a particular address.

- **wfl**
  Displays the PCF summary in a single very wide line.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. Please refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference* for details on the usage of `grep` and `more`.

**Usage**

Use this command to display a summary of all PCFs.

**Example**

```
show session counters pcf-summary
```
show session disconnect-reasons

Displays a list of the reasons for call disconnects and the number of calls disconnected for each reason.

Product
All

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

show session disconnect-reasons [ gprs-only | sgsn-only | mme-only | verbose ] [ [ grep [ grep_options ] | more ] ]

- **gprs-only**
  Only supported on the SGSN.
  This keyword limits the display to session disconnect reasons for the SGSN’s 2G MM and PDP context disconnects.

- **sgsn-only**
  Only supported on the SGSN.
  This keyword limits the display to session disconnect reasons for the SGSN’s 3G MM and PDP context disconnects.

- **mme-only**
  This keyword filters to the list of the session disconnect reasons for MME call disconnects.

- **verbose**
  List all disconnect reasons even if the values are zero (0).

- **grep [ grep_options ] | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to display a list of the reasons why calls were disconnected.

Example

To view session disconnect statistics, enter the following command:

```
show session disconnect-reasons
```

To view a list of the disconnect reasons with verbose output, enter the following command:
show session disconnect-reasons verbose

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show session duration

Displays session duration information for the current context filtered by the options specified.

**Product**
All

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Syntax**

```
show session duration [ session_filter ] [ | { grep grep_options | more } ]
```

**session_filter**

Indicates name of the sessions/services/AGWs whose session duration information is to be filtered and displayed. This consist of following:

- **asn-peer-address ip_address**: Indicates that only the session information for the ASN GW peer whose IP address is specified by `ip_address` is to be displayed. `ip_address` must be specified using the standard IPv4 dotted decimal notation.

- **asnsgw-service service_name**: Indicates that only the session information for the ASN GW service whose name is specified by `service_name` is to be displayed.

- **asnpc-peer-address ip_address**: Indicates that only the session information for the ASN PC peer whose IP address is specified by `ip_address` is to be displayed. `ip_address` must be specified using the standard IPv4 dotted decimal notation.

- **asnpc-service service_name**: Indicates that only the session information for the ASN PC service whose name is specified by `service_name` is to be displayed.

- **apn apn_name**: Indicates that only session information for the specified APN will be displayed. `apn_name` specifies the name of a configured APN that can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **cscf-service service_name**: Indicates that only session information for the specified CSCF service will be displayed. `service_name` must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

**Important**: CSCF SIP calls under progress only. Registrations will not be considered a call.

- **dhcp-server dhcp_address**: Indicates that only session information for the specified DHCP server will be displayed. `dhcp_address` is the name of the DHCP server and must be expressed in dotted decimal notation.

- **fa fa_address**: indicates only the session information for the foreign agent whose IP address is specified by `fa_address` is to be displayed. `fa_address` must be specified using the standard IPv4 dotted decimal notation.

- **fa-service fa_name**: indicates only the session information for the foreign agent service specified by `fa_name` is to have information displayed.

- **ggsn-service ggsn_name**: Indicates that only session information for the specified GGSN service will be displayed. `ggsn_name` specifies the name of a configured GGSN service that can be from 1 to 63 alpha and/or numeric characters and is case sensitive.
• **gprs-only**: Limits the display to the session information for the SGSN’s 2G MM and PDP contexts.

• **ha ha_address**: indicates only the session information for the home agent whose IP address is specified by ha_address is to be displayed. ha_address must be specified using the standard IPv4 dotted decimal notation.

• **ha-service ha_name**: indicates only the session information for the home agent service specified by ha_name is to be displayed.

• **hsgw-service service_name**: indicates only the session information for the HSGW service specified by the service_name is to be displayed. service_name must be an existing HSGW service and be from 1 to 63 alpha and/or numeric characters.

• **lma-service service_name**: indicates only the session information for the LMA service specified by the service_name is to be displayed. service_name must be an existing LMA service and be from 1 to 63 alpha and/or numeric characters.

• **mme-service service_name**: indicates only the session information for the MME service specified by the service_name is to be displayed. service_name must be an existing MME service and be from 1 to 63 alpha and/or numeric characters.

• **mag-service service_name**: indicates only the session information for the MAG service specified by the service_name is to be displayed. service_name must be an existing MAG service and be from 1 to 63 alpha and/or numeric characters.

• **pcf pcf_address**: indicates only the session information for the packet control function with IP address pcf_address is to be displayed. pcf_address must be specified using the standard IPv4 dotted decimal notation.

• **pdsn-service pdsn_name**: indicates only the session information for the packet data service specified by pdsn_name is to have information displayed.

---

**Important**: If no PCF address or PDSN service is specified the session information for all sessions is displayed.

• **sgsn-address sgsn-address**: Indicates that only session information for the specified SGSN will be displayed. sgsn_address is the IP address of the SGSN and must be expressed in dotted decimal notation.

• **sgsn-only**: Limits the display to the session information for the SGSN’s 3G MM and PDP contexts.

• **sgw-service service_name**: indicates only the session information for the S-GW service specified by the service_name is to be displayed. service_name must be an existing S-GW service and be from 1 to 63 alpha and/or numeric characters.

---

```bash
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of **grep** and **more**, refer to the **Regulating a Command’s Output** section of the **Command Line Interface Overview** chapter in the **Command Line Interface Reference**.

---

**Usage**

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.
Example
The following commands display the duration information for the session connected to the packet control function with address 1.2.3.4, packet data service sampleService, and for all sessions, respectively.

```
show session duration pcf 1.2.3.4
show session duration pdsn-service sampleService
show session duration
```

The following is a sample of the output.

```
In-Progress Call Duration Statistics <1min 3 <2min 44 <5min 126 <15min 32 <1hr 3 <4hr 1 <12hr 0 <24hr 0 >24hr 0
```

The column on the left lists various time intervals ranging from less than (<) 1 minute to greater than (>) 24 hours. The column on the right categorizes the number subscriber sessions that are currently in progress into the appropriate time interval.
show session progress

Displays session progress information for the current context filtered by the options specified.

**Product**
All

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Syntax**

```
show session progress [ asn-peer-address ip_address | asngw-service service_name | asnpc-service service_name | asnpc-peer-address ip_address | apn apn_name | csfc-service service_name | dhcp-server dhcp_address | fa fa-address | fa-service fa_name | ggsn-service ggsn_name | ha ha_address | ha-service ha_address | hsgw-service service_name | lma-service service_name | mag-service service_name | mme-address mme_address | pcf { pcf_address | all } | pdsn-service pdsn_name | pgw-address ip_address | sgsn-address sgsn_address | sgw-service service_name ] [ | | { grepgrep_options | more } ]
```

**progress**: indicates session progress information is to be displayed.

- **asn-peer-address ip_address**: Indicates that only the session information for the ASN GW peer whose IP address specified by *ip_address* is to be displayed. *ip_address* must be specified using the standard IPv4 dotted decimal notation.

- **asngw-service service_name**: Indicates that only the session information for the ASN GW service whose name is specified by *service_name* is to be displayed.

- **asnpc-service service_name**: Indicates that only the session information for the ASN PC service whose name is specified by *service_name* is to be displayed.

- **asnpc-peer-address ip_address**: Indicates that only the session information for the ASN PC peer whose IP address specified by *ip_address* is to be displayed. *ip_address* must be specified using the standard IPv4 dotted decimal notation.

- **apn apn_name**: Indicates that only session information for the specified APN will be displayed. *apn_name* specifies the name of a configured APN that can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **csfc-service service_name**: Indicates that only session information for the specified CSCF service will be displayed. *service_name* must be an existing CSCF service and be from 1 to 63 alpha and/or numeric characters.

***Important***: CSCF SIP calls under progress only. Registrations will not be considered a call.
Exec Mode Show Commands (Q-S)

**show session progress**

- **dhcp-server dhcp_address**: Indicates that only session information for the specified DHCP server will be displayed. *dhcp_address* is the name of the DHCP server and must be expressed in dotted decimal notation.

- **fa fa_address**: indicates only the session information for the foreign agent whose IP address is specified by *fa_address* is to be displayed. *fa_address* must be specified using the standard IPv4 dotted decimal notation.

- **fa-service fa_name**: indicates only the session information for the foreign agent service specified by *fa_name* is to have information displayed.

- **ggsn-service ggsn_name**: Indicates that only session information for the specified GGSN service will be displayed. *ggsn_name* specifies the name of a configured GGSN service that can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **ha ha_address**: indicates only the session information for the home agent whose IP address is specified by *ha_address* is to be displayed. *ha_address* must be specified using the standard IPv4 dotted decimal notation.

- **ha-service ha_name**: indicates only the session information for the home agent service specified by *ha_name* is to have information displayed.

- **hsgw-service service_name**: Indicates only the session progress information for the HSGW service specified by the *service_name* is to be displayed. *service_name* must be an existing HSGW service and be from 1 to 63 alpha and/or numeric characters.

- **lma-service service_name**: Indicates only the session progress information for the LMA service specified by the *service_name* is to be displayed. *service_name* must be an existing LMA service and be from 1 to 63 alpha and/or numeric characters.

- **mag-service service_name**: Indicates only the session progress information for the MAG service specified by the *service_name* is to be displayed. *service_name* must be an existing MAG service and be from 1 to 63 alpha and/or numeric characters.

- **mme-address mme_address**: indicates only the session information for the foreign agent whose IP address is specified by *mme_address* is to be displayed. *mme_address* must be specified using the standard IPv4 dotted decimal notation.

- **pcf pcf_address**: Indicates only the session information for the packet control function with IP address *pcf_address* is to be displayed. *pcf_address* must be specified using the standard IPv4 dotted decimal notation.

- **pcf all**: indicates the session information for the packet control function for all pcf addresses.

- **pdsn-service pdsn_name**: indicates only the session information for the packet data service specified by *pdsn_name* is to have information displayed.

---

**Important:** If no PCF address or PDSN service is specified the session information for all sessions is displayed.

- **pgw-address ip_address**: Indicates only session progress information for the P-GW with an IP address specified by *ip_address* is to be displayed. *ip_address* must be specified using the standard IPv4 dotted decimal notation.

- **sgsn-address sgsn-address**: Indicates that only session information for the specified SGSN will be displayed. *sgsn-address* is the IP address of the SGSN and must be expressed in dotted decimal notation.
show session progress

**sgw-service service_name**: Indicates only the session progress information for the S-GW service specified by the **service_name** is to be displayed. **service_name** must be an existing S-GW service and be from 1 to 63 alpha and/or numeric characters.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**
View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

**Example**
The following commands display the status information for the session connected to the packet control function with address 1.2.3.4, packet data service **sampleService**, and for all sessions, respectively.

```bash
show session progress pcf 1.2.3.4
show session progress pdsn-service sampleService
show session progress
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show session recovery status

Displays session recovery status information for the current context filtered by the options specified.

Product
All

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

```
show session recovery status [verbose] [ | { grep grep_options | more } ]
```

---

recovery status
Displays the current status of the system’s ability to recover from a hardware or software fault that requires the recovery of home agent-based Mobile IP session(s).

verbose
Includes per-CPU Session Recovery status.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

---

Usage
View the session information for troubleshooting subscriber problems and for general monitoring for orphaned sessions.

---

Example
To display the session recovery status information, enter the following command:

```
show session recovery status
```

Adding the optional verbose keyword to this command provides more details.

```
show session recovery status verbose
```

---

`Important:` Output descriptions for commands are available in the Statistics and Counters Reference.
show session setuptime

Displays session setup time information for all sessions or sessions associated with the specified AGW/node.

Product
All

Privilege
Operator

Syntax

```
show session setuptime [ mme-only | pcf pcf_address | gprs-only | sgsn-address sgsn-only ] [ | { grep grep_options | more } ]
```

Displays the call setup times aggregated into basic ranges of time.
- **mme-only**: Filters and displays the call setup information for MME calls only.
- **pcf pcf_address**: displays call setup data for the packet control function whose IPv address is specified as `pcf_address.pcf_address` must be specified using the standard IPv4 dotted decimal notation. The call setup times for all PCFs is displayed when no specified PCF is specified.
- **gprs-only**: Displays 2G call setup data for the for the SGSN for the MM and PDP contexts.
- **sgsn-address sgsn_address**: Displays call setup times for the specified SGSN.
  - `sgsn_address` is the IP address of the SGSN and must be expressed in dotted decimal notation. This keyword is used by the GGSN.
- **sgsn-only**: Displays 3G call setup data for the for the SGSN for the MM and PDP contexts.

```
| grep grep_options | more |
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

Usage

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

When no keywords are specified, the information shown is cumulative for all sessions that have been facilitated by the system.

Example

The following command shows setup time statistics for all sessions from the PCF at IP address 192.168.10.3:

```
show session setuptime pcf 192.168.10.3
```
show session subsystem

Displays session information for system subsystems. If no keywords are specified, information for all subsystems is displayed.

Product
All

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

show sessionsubsystem [ full | facility facility [ all | instanceid ] ] [ verbose ] [ | { grep grep_options | more }]

[ full | facility facility [ all | instance id ] ]

• full: Indicates that a full statistics summary of all subsystems is to be displayed.
• facility facility: Specifies the facility for which subsystem statistics is to be displayed where facility is specified as one of:
  • a11mgr: A11 Manager
  • aaamgr: Accounting and Authentication Manager
  • aaaprox: AAA Proxy Manager
  • asngwmgr: ASN Gateway Manager
  • asnpcmgr: ASN Paging/Location-Registry Manager
  • cscfmgr: SIP CSCF Manager
  • dgmbmgr: Diameter Gmb Application Manager
  • diamsproxy: Diameter Proxy Application Manager
  • egtpegmgr: EGTP Egress Demux Manager
  • egtpinmgr: EGTP Ingress Demux Manager
  • famgr: Foreign Agent Manager
  • gtpumgr: GTPUMGR Demux Manager
  • gtpcmgr: GTPC Manager
  • hambmgr: Home Agent Manager
  • hnbmgr: HNBGW HNB Manager
  • imsimgr: SGSN IMSI Manager
  • ipsgmgr: IP Services Gateway Manager
  • l2tudemux: L2TP Demux Manager
  • l2tpmgr: L2TP Manager
  • linkmgr: SGSN/SS7 Master Manager
  • magmgr: Mobile Access Gateway Manager
Exec Mode Show Commands (Q-S)

show session subsystem

- `megadiammgr`: Mega Diameter Manager
- `mmedemux`: MME Demux Manager logging facility
- `mmemgr`: MME Manager logging facility
- `mmgr`: SGSN/SS7 Master Manager
- `phsgwmgr`: PHS Gateway Manager
- `phspcmgr`: PHS Paging Controller Manager
- `sessmgr`: Session Manager
- `sgtpcmgr`: SGSN GTPC Manager

- `all` | `instance id` the keyword `all` indicates all instances of the specified facility are to be displayed whereas the keyword `instance` specifies a specific instance for which information is to be displayed where `id` must be specified as an instance ID in the range 0 through 4294967295. If `all` or `instance` is not specified summary statistics are displayed.

verbose
Displays everything the show session subsystem command output displays with the exception that the Setup Time statistics are reported in 100 ms increments from <100 ms up to 9600 ms.

`grep grep_options | more`
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. Please refer to the Regulating the Command Output section in the Command Line Interface Reference for details on the usage of `grep` and `more`.

Usage
View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.
If this command is entered with no keywords, the information displayed is cumulative for all sessions facilitated by the system.

Example
The following commands display the statistics information summarized for all sessions, then for the `fgmgr` facility (all sessions), and finally only for the session with ID 127589 for the `hamgr` subsystem.

```
  show session subsystem full
  show session subsystem facility allmgr all
  show session subsystem facility aaamgr all
  show session subsystem facility asngwmgmt all
  show session subsystem facility fngmgr all
  show session subsystem facility hamgr all
  show session subsystem facility sessmgr all
```
show session subsystem facility aaaproxy all

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
**show session trace**

Displays status and statistics for the session trace application.

**Product**
MME, P-GW, S-GW

**Privilege**
Inspector

**Syntax**

```
show session trace { statistics | subscriber network-element { mme | pgw | sgw } trace-ref value | tce-address ip_address tce-index num | tce-summary | trace-summary } [ | { grep grep_options | more } ]
```

- **statistics**
  Displays summary statistics of the session trace subsystem.

- **subscriber network-element { mme | pgw | sgw } trace-ref value**
  Displays status and statistics of a specified session trace using the network element type and the trace reference. `value` must be a valid trace reference 12 characters in length.

- **tce-address ip_address tce-index num**
  Displays status and statistics of a specified Trace Collection Entity (TCE) connection. `ip_address` must be a valid existing collection entity IPv4 address and is specified in dotted decimal notation.

- **tce-summary**
  Displays a summary of all active TCE connections.

- **trace-summary**
  Displays a summary of all active session traces.

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. Please refer to the Regulating the Command Output section in this reference for details on the usage of `grep` and `more`.

**Usage**
Use this command to display status and statistics for the session trace application.

**Example**
The following command displays status and statistics for a subscriber session trace on a P-GW with a trace reference of 32223398765:
show session trace subscriber network-element pgw trace-ref 32223398765

The following command displays status and statistics for a subscriber session trace on an MME with a trace reference of 32221234567:

```
show session trace subscriber network-element pgw trace-ref 32223398765
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show sgsn-operator-policy

Displays configuration information for the SGSN features bundled into the SGSN Operator Policy and includes operational configuration for features such as GPRS Attach, GPRS RAU Inter, and PTMSI-Realloc Service Request (Signalling).

Product
SGSN

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

```
show sgsn-operator-policy ( all | full | name op-pol-name ) +
```

- **all**
  Displays information for all configured SGSN operator policies.

- **full**
  Display all details of the configuration for the specified SGSN Operator Policy.

- **name op-pol-name**
  Identifies a specific operator policy. `op-pol-name` must be a combination of 1 to 64 alphanumeric characters.

Usage
This command can be used to display all of the operator policies that have been configured or all of the configuration information for a specific operator policy.

Example
The following command displays information for all configured SGSN operator policies:

```
show sgsn-operator-policy all
```
show sgsn-service

This command displays information about the configured SGSN services in the current context.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Syntax**

```bash
show sgsn-service { all | name svc_name }
```

- `all`
  Displays information for all SGSN services in the current context.

- `name svc_name`
  Displays information for the specified SGSN service in the current context. `svc_name` must be the name of a configured SGSN service and must be an alphanumeric string from 1 to 63 characters in length.

**Usage**

Use this command to display information for SGSN services.

**Example**

The following command displays information for all SGSN services in the current context:

```bash
show sgsn-service all
```

The following command displays information for an SGSN service in the current context that is named sgsn1:

```bash
show sgsn-service name sgsn1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show sgsn sessmgr

This command displays session manager (SMGR) statistics specific to the SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

show sgsn sessmgr { all | instance }

---

**all memory statistics**
Displays all SMGR statistics specific to the system’s SGSN service.

---

**instance smgr_inst memory statistics**
Displays the statistics for a specific session manager instance of the SGSN service. 
*smgr_inst* must be an integer between 1 and 10000000.

---

Usage
Use this command to display information for SGSN services.

---

Example
The following command displays GPTP-U statistics for the traffic between an SGSN and a connected RNC.

```
show sgtpu statistics rnc-address 123.1.2.3
```
show sgtp-service

This command displays information about the configured SGTP services in the current context, including GTP-C and GTP-U operational configuration.

**Product**
SGSN
PDG/TTG

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Syntax**

```
show sgtp-service { all | ggsn-table | sgsn-table | name svc_name }
```

- **all**
  Displays configuration information for all of the SGTP services defined for the current context.

- **ggsn-table**
  Displays GGSN information configured for the SGTP service in the current context.

- **sgsn-table**
  Displays SGSN information configured for the SGTP service in the current context.

- **name svc_name**
  Displays information for the specified SGTP service in the current context. *svc_name* must be the name of a configured SGTP service and must be an alphanumeric string from 1 to 63 characters in length.

**Usage**

Use this command to display information for SGSN services.

**Example**
The following command displays information for all SGTP services in the current context:

```
show sgtp-service all
```

The following command displays the GGSN information in SGTP services in the current context:

```
show sgtp-service ggsn-table
```

The following command displays the SGSN information in SGTP services in the current context:

```
show sgtp-service sgsn-table
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show sgtp-service
show sgtpc statistics

This command displays all statistics, for SGTPC interface parameters, collected since the last restart or last use of a clear command.

Product
SGSN
PDG/TTG

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

```
show sgtpc statistics [ all | gsn-address ipv4_address | sgtp-service sgtp_svc_name ] [ verbose ]
```

**all**
Displays configuration information for all of the SGTP services defined for the current context.

**gsn-address ipv4_address**
`ipv4_address` Displays statistics for a specific SGSN identified by the SGSN’s IPv4 address. specified in dotted decimal notation.
Note this must be an existing and active interface.

**sgtp-service sgtp_svc_name**
Displays statistics for the specified SGTP service in the current context.
`sgtp_svc_name` must be the name of a previously configured and active SGTP service and must be an alphanumeric string from 1 to 63 characters in length.

**verbose**
Causes the system to display a more detailed level of statistics.

Usage
Use this command to display information for SGSN services.

Example
The following command displays statistics for the SGTP service named `sgtp1`:

```
show sgtpc statistics sgtp-service sgtp1
```

**Important:** Output descriptions for commands are available in the `Statistics and Counters Reference`.
show sgtpu statistics

This command displays all transmission and reception statistics, for pre-defined and active GTP-U interfaces, collected since the last restart or last use of a clear command.

Product
SGSN
PDG/TTG

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

show sgtpu statistics [ ggsn-address ipv4_address | iups-service iups_srvc_name | rnc-address ipv4_address | sgtp-service sgtp_srvc_name | gprs-service gprs_srvc_name nsei nse_id ]

  ggsn-address ipv4_address
  ipv4_address Displays statistics for a specific GGSN identified by the GGSN’s IPv4 address. specified in dotted decimal notation.

  iups-service iups_srvc_name
  Displays statistics for the specified IuPS service in the current context.
  iups_srvc_name must be the name of a previously configured and active IuPS service and must be an alphanumeric string from 1 to 63 characters in length.

  rnc-address ipv4_address
  ipv4_address Displays statistics for a specific RNC identified by the RNC’s IPv4 address. specified in dotted decimal notation.

  sgtp-service sgtp_srvc_name
  Displays statistics for the specified SGTP service in the current context.
  sgtp_srvc_name must be the name of a previously configured and active SGTP service and must be an alphanumeric string from 1 to 63 characters in length.

  gprs-service gprs_srvc_name nsei nse_id
  Displays the statistics for a specific NSEI-based GTPU statistics associated with the specified GPRS service in the current context.
  gprs_srvc_name must be the name of a previously configured and active GPRS service and must be an alphanumeric string from 1 to 63 characters in length.
  nsei nse_id must be an integer from 0 to 65535.

Usage

Use this command to display information for SGSN services.
Example
The following command displays GPTP-U statistics for the traffic between an SGSN and a connected RNC.

```
show sgtpu statistics rnc-address 123.1.2.3
```
**show sgw-service**

Displays configuration information and/or service statistics for Serving Gateway (S-GW) services on this system.

**Product**
S-GW

**Privilege**
Inspector

**Syntax**

```
show sgw-service { all | name service_name } statistics { all | name service_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays configuration information for all S-GW services configured on this system.

- **name service_name**
  Displays configuration information for a specific S-GW service configured on this system. `service_name` must be an existing S-GW service, and be from 1 to 63 alpha and/or numeric characters in length.

- **statistics { all | name service_name }**
  Displays statistics for all S-GW services on this system or for a specified service. `service_name` must be an existing S-GW service and be from 1 to 63 alpha and/or numerics characters.

  | { grep grep_options | more }
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

  For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view configuration information and/or service statistics for S-GW services on this system.

**Example**

The following command displays service statistics for the S-GW service named `sgw1`:

```
show sgw-service statistics name sgw1
```
show snmp

Displays information on the Simple Network Management Protocol servers and interfaces.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show snmp { accesses | communities | contexts | notifies | server | transports | trap [ history | statistics ] | views } [ | { grep grep_options | more } ]

accesses
Displays SNMP server usage statistics.

communities
Displays SNMP community strings.

contexts
Displays SNMP information per context.

notifies
Displays SNMP event trap and notification statistics.

server
Displays SNMP server configuration information.

transports
Displays trap destination configuration information.

trap [ history | statistics {verbose}{wide}]

history: displays SNMP event trap history. trap history shows up to 5000 time-stamped trap records stored in a buffer. The buffer may be cleared by entering the clear snmp history command.
statistics: displays SNMP event trap and notification statistics.
verbose: displays rows for every defined trap, even if never generated.
wide: shows trap statistics data in excess of 80 columns.

views
Displays SNMP views.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage

Display SNMP information as part of system verification and troubleshooting.

### Example

The following commands display the usage statistics, community string information, event trap and notification data, server information, and trap destination configuration, respectively.

```
show snmp communities
show snmp transport
show snmp server
show snmp accesses
show snmp notifies
show snmp trap history
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show srp

Displays the Service Redundancy Protocol information.

Product
HA, PDSN GGSN PDIF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show srp { call-loss statistics | checkpoint statistics [ verbose ] | info | statistics } | [ grep grep_options | more ]
```

- **call-loss statistics**
  Displays history of lost calls during switchover.

- **checkpoint statistics [ verbose ]**
  Displays checkpointing statistics on session redundancy data (session managers, current call recovery records, etc.).
  - **verbose**: Displays cumulative information for all session managers in tabular output.

- **info**
  Displays Service Redundancy Protocol information (context, chassis state, peer, connection state, etc.).

- **statistics**
  Displays Service Redundancy Protocol statistics (hello messages sent, configuration validation, resource messages, switchovers, etc.).

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of `grep` and `more`, refer to the `Regulating a Command's Output` section of the `Command Line Interface Overview` chapter in the `Command Line Reference`.

Usage
The output of this command may be considered as part of a periodic system auditing program by verifying the Service Redundancy Protocol performance. For more information, refer to the Interchassis Session Recovery chapter of the Administration and Configuration Guide and the Service Redundancy Protocol Configuration Mode chapter of the Command Line Reference.

Example
The following command shows Service Redundancy Protocol information:
show srp call-loss statistics
show srp info
show srp checkpoint statistics
show srp statistics

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show srp monitor

Displays the Service Redundancy Protocol monitor information.

Product
HA, GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show srp monitor [ all | authentication-probe | bgp | [ grep grep_options | more ] ]
```

<table>
<thead>
<tr>
<th>all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays monitor information for all types (authentication-probe and bgp).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>authentication-probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays authentication probe monitor information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bgp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays BGP monitor statistics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>grep grep_options</th>
<th>more</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of <code>grep</code> and <code>more</code>, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.</td>
<td></td>
</tr>
</tbody>
</table>

Usage
The output of this command may be considered as part of a periodic system auditing program by verifying the Service Redundancy Protocol performance. For more information, refer to the Interchassis Session Recovery chapter of the Administration and Configuration Guide and the Service Redundancy Protocol Configuration Mode chapter of the Command Line Reference.

Example
The following command shows Service Redundancy Protocol monitor information:

```
show srp monitor
```
show ss7-routing-domain

This command displays the configuration information for the defined SS7 routing domains. As SS7 routing domains conglomerate a large number of operational parameters, this command enables you to narrow your displays to specific protocol parameters on a specific link.

Product
SGSN

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

```
show ss7-routing-domain { all | ss7rd_id { m3ua | mtp2 | mtp3 | qsaal | routes [ adjacent ] } | sctp asp { all | instance asp_id } | ssf } }

show ss7-routing-domain ss7rd_id m3ua { statistics { gen | peer-server { all | id peer-server_id peer-server-process { all | instance psp_instance } } } | status { address-translation-table | destination-point-code { all | ss7_dpc } | gen | peer-server peer-server_id [ peer-server-process instance psp_id | verbose ] } }

show ss7-routing-domain 1 ssf { statistics linkset { all | id linkset_id link { all | id link_id } } | status linkset { all | id linkset_id link { all | id link_id [ verbose ] } } }
```

```
ss7-routing-domain { all | ss7rd_id }
```

Specifies whether the display will output information for all SS7 routing domains or only for a specifically identified SS7 routing domain.

`ss7rd_id` must be an integer value from 1 through 12.

```
m3ua
```

Provides access to statistics or status information for the SS7 MTP3 User Adaptation Layer (M3UA) the specified SS7 routing domain.

```
mtp2
```

Provides access to statistics or status information the SS7 Message Transfer Part-2 (MTP2) for the specified SS7 routing domain.

```
mtp3
```

Provides access to statistics or status information the SS7 Message Transfer Part-3 (MTP3) for the specified SS7 routing domain.

```
qsaal
```

Provides access to statistics or status information for the Service Specific Connection-Oriented Protocol (SSCOP) sub-layer of the Quasi Signaling Application Adaptation Layer (QSAAL) for the specified SS7 routing domain.
**routes [ adjacent ]**

Displays the destination point code (DPC) routing table.
adjacent - If this keyword is used with the routes keyword, then it provides access to the statistics and status information for configured adjacent point codes.

**sctp asp [ all | instance asp_id ]**

Provides access to the status or statistics of Stream Control Transmission Protocol (SCTP) application server processes (ASP) in the specified SS7 routing domain for all or a specified SCTP ASP instance.
- **all**: This keyword displays the information for all SCTP application server process instances for specific SS7 routing domain.
- **instance asp_id**: Specified the specific SCTP application server process instance where
  \[ instance_id \] must be an integer value from 1 through 4.

**sscf**

Provides access to the statistics or status information for the Service Specific Coordination Function (SSCF (q.2140)) for the specified SS7 routing domain.

**peer-server [ all | id peer-server_id ]**

This keyword filters the information for the specific protocol in SS7 routing domain for all or specific peer server id.
- **all**: This keyword displays the information for all peer servers for specific protocol.
- **id peer-server_id**: Specified the specific linkset identifier where \( peer-server_id \)must be an integer value from 1 through 49.

**peer-server-process [ all | instance instance_id ]**

This keyword filters the information for the specific protocol in SS7 routing domain for all or specific instance of peer-server process.
- **all**: This keyword displays the information for all peer server process instances for specific protocol.
- **instance instance_id**: Specified the specific peer server process instance where
  \[ instance_id \] must be an integer value from 1 through 4.

**destination-point-code [ all | dest_point_code ]**

This keyword filters the information for the specific protocol in SS7 routing domain for all or specific destination point code.
- **all**: This keyword displays the information for all destination point codes in SS7 routing domain.
- **dest_point_code**: Specified the specific destination point code in SS7 routing domain.

**gen**

This keyword displays the general information for the specific protocol for the specified SS7 routing domain.

**verbose**

This keyword enables the display of maximum information for a protocol statistics/status.
```
linkset [ all | id linkset_id ]
This keyword filters the information for the specific protocol in SS7 routing domain for all or specific link set.
- **all**: This keyword displays the information for all linksets for specific protocol.
- **id linkset_id**: Specified the specific linkset identifier where linkset_id must be an integer value from 1 through 49.

link [ all | id link_id ]
This keyword filters the information for the specific protocol in SS7 routing domain for all or specific link set.
- **all**: This keyword displays the information for all links for specific protocol.
- **id link_id**: Specified the specific linkset identifier where link_id must be an integer value from 1 through 16.

Usage
Use this command to display the SS7 routing domain and different layer protocol information for SGSN service.

Example
Following command displays the information/statistics of all SCTP application server processes of peer server id 17 and peer server process instance 1 in SS7 routing domain 12:

```
show ss7-routing-domain 12 sctp asp all status peer-server id 17 peer-server-process instance 1
```

> **Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show ssh key

Displays the secure shell public key information.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ssh key [ type { v1-rsa | v2-rsa | v2-dsa } ] [ | { grep grep_options | more } ]
```

| type { v1-rsa | v2-rsa | v2-dsa } |
|-----------------------------|
| Specifies the type of SSH key information to display. If type is not specified, information for all types is displayed. |
| v1-rsa: SSH v1 RSA host key only |
| v2-rsa: SSH v2 DSA host key only |
| v2-dsa: SSH v2 RSA host key only |

`grep grep_options | more`

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter in the `Command Line Interface Reference`.

Usage
Show the secure shell key information for all types to verify installed keys.

Example
The following command shows information for all SSH V1 and SSH V2 keys:

```
show ssh key
```

The following command shows information for only SSH V2 RSA host keys:

```
show ssh key type v2-rsa
```
show subscribers

Shows information for subscriber sessions defined by the specified keywords. Keywords described under Command Keywords below are base commands that display distinctive type of data. Keywords described under Filter Keywords are filters that modify or filter the output of the base commands. Not all filter keywords are available for all command keywords commands. Each command keyword lists the filter keywords that it accepts.

Product
All

Privilege
Security Administrator, Administrator, Inspector, Operator

Syntax

```
show subscribers [ command_keyword ] [ filter_keywords ] [ | { grep grep_options | more } ]
```

Command Keywords

The following keywords are base commands that each have a distinct display output. Only one Command Keyword can entered on the command line.

```
aaa-configuration
```

Shows AAA configuration information for subscriber sessions defined by the specified filter keywords. The following filter keywords are valid with this command:

- `active`, `all`, `apn`, `callid`, `card-num`, `configured-idle-timeout`, `connected-time`, `dhcp-server`, `dormant`, `fa`, `fa-service`, `ggsn-service`, `ha`, `ha-service`, `idle-time`, `imsi`, `ip-address`, `ip-pool`, `lac`, `lac-service`, `lns`, `lns-service`, `long-duration-time-left`, `msid`, `network-requested`, `network-type`, `pcf`, `pdsn-service`, `plmn-type`, `rx-data`, `session-time-left`, `sgsn-address`, `sgsn-service`, `tx-data`, `username`, `verbose`, `grep`, `more`

```
access-flows { accounting | dynamic | pre-provisioned | static }
```

Shows the ip-flows for the subscribers defined by the specified filter keywords.

- `accounting`: Use this keyword to display the accounting type of access flows for a subscriber.
- `dynamic`: Use this keyword to display the dynamic type of access flows for a subscriber.
- `pre-provisioned`: Use this keyword to display the pre-provisioned type of access flows for a WiMAX subscriber.
- `static`: Use this keyword to display the static type of access flows for a subscriber.

The following filter keywords are valid with this command:

- `active`, `active-charging-service`, `all`, `asngw-service`, `asnp-service`, `asnp-peer-address`, `apn`, `callid`, `card-num`, `ccoa-only`, `configured-idle-timeout`, `connected-time`, `dhcp-server`, `dormant`, `fa`, `fa-service`, `flow-type`, `ggsn-service`, `gsm-traffic-class`, `ha`, `ha-ipsec-only`, `ha-service`, `idle-time`, `imsi`, `ip-address`, `ip-pool`, `ipv6-address`, `ipv6-prefix`, `13-tunnel-local-address`, `13-tunnel-remote-address`, `lac`, `lac-service`, `lns`, `lns-service`, `long-duration-time-left`, `mip-udp-tunnel-only`, `msid`, `msiddn`, `network-requested`, `network-type`, `pcf`, `pdsn-service`, `plmn-type`, `rulebase`, `rx-data`,...
Exec Mode Show Commands (Q-S)

show subscribers

Display subscribers link activity percentage. When no Filter Keywords are specified, the output is a summary of all subscriber activity. When Filter Keywords are specified, the link activity percentage is displayed as graphs in which one is displayed using a high sampling rate, a 10 second interval between samples, and a low sampling rate, a 15 minute interval between samples.

The following filter keywords are valid with this command:

active, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant, fa, fa-service, ggsn-service, ha, ha-service, idle-time, imsi, ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-time-left, msid, network-requested, pcf, pdns-service, plmn-type, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

asn-peer-address ip_address

Displays information for subscribers on an ASN GW trusted peer.

ip_address is the IPv4 address of the ASN GW peer server in dotted decimal notation.

The following filter keywords are valid with this command:

all, counters all, asngw-service, full, summary, grep, more

asngw-service service_name

Displays counters for subscribers accessing the ASN GW service.

service_name must be an existing service and be from 1 to 63 alpha and/or numeric characters in length.

The following filter keywords are valid with this command:

all, counters all, full, summary, grep, more

asnpc-service service_name

Displays counters for subscribers accessing the ASN Paging Controller and Location Registry service.

service_name must be an existing ASN PC service and be from 1 to 63 alpha and/or numeric characters in length.

The following filter keywords are valid with this command:

all, counters all, full, summary, grep, more

bearer-establishment { direct-tunnel | normal | pending }  

Selects Bearer Establishment type defined by the specified filter keywords.

direct-tunnel: Select subscribers having direct tunnel established with the RNC.
normal: Select subscribers having bearer established with SGSN.
pending: Select subscribers for whom bearer is not fully established.

configuration

Display current configuration for all subscribers or a specified subscriber. The following filter keywords are valid with this command:
**show subscribers**

**counters**
Show the counters associated with the subscriber. The following filter keywords are valid with this command:
active, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant, fa, fa-service, ggsn-service, ha, ha-service, idle-time, imsi, ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-time-left, msid, network-requested, network-type, pcf, pdsn-service, plmn-type, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

**cscf-only**
Displays information for CSCF subscribers only.
The following filter keywords are valid with this command:

```
aaa-configuration, access-flows, active, activity, all, bearer-establishment, callid, card-num, configured-idle-timeout, connected-time, counters, cscf-service, data-rate, dormant, fa, full, gtp-version, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, network-type, policy, rx-data, session-time-left, smgr-instance, subscription, summary, tft, tx-data, username, wfl
```

**cscf-service service_name**
Displays information for subscribers accessing the specified CSCF service.
`service_name` must be an existing service and be from 1 to 63 alpha and/or numeric characters in length.
The following filter keywords are valid with this command:

```
bearer-establishment, callid, card-num, configured-idle-timeout, connected-time, cscf-service, fa, gtp-version, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, network-type, rx-data, session-time-left, smgr-instance, subscription, tx-data, username
```

**css-delivery-sequence**

**Important:** This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

**css-service csssvc_name**

**Important:** This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

**data-rate [ summary | full ] [ verbose | graph { high | low } ] [ high | low ]**
Indicates how to display subscriber throughput data.
**Important:** This keyword is best used for individual subscriber output.

**summary** Combine statistics for the matching subscriber and show a summary in text form.

**full** Display a separate output for each matching subscriber separately in tabular form.

**verbose** Display cumulative information for all matching subscribers in tabular output.

**graph** \{**high** | **low** \}: Display the throughput data as a graph using either a high sampling rate of every 30 seconds or a low sampling rate of every 15 minutes. The graph contains data points over the last 24 hours, if available. The command displays a graph each for the transmit and receive peak, average, and sustained throughput for a total of six graphs.

**high** Display the raw data collected for the throughput analysis using a high sampling rate (smaller interval). The data displayed uses a sampling interval of 30 seconds and includes the data collected over the last 24 hours, if available.

**low** Display the raw data collected for the throughput analysis using a low sampling rate (larger interval). The data displayed uses a sampling interval of 15 minutes and includes the data collected over the last 24 hours, if available.

The following filter keywords are valid with this command:

- active, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant, fa, fa-service, ggsn-service, ha, ha-service, hsgw-only, hsgw-service, idle-time, imsi, ip-address, ip-pool, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, network-requested, pcf, pdsn-service, plmn-type, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

**debug-info** \{**callid** id | **msid** id | **username** name \}

Displays internal call troubleshooting information for subscriber sessions defined by the specified keywords.

**callid** id: Displays subscriber information for the call specified by **id**. The call ID must be specified as an 8-byte hexadecimal number.

**msid** id: Displays information for the mobile user identified by **id**. The **id** must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (’). For example: ‘$’.

**username** name: Displays information for connections for the subscriber identified by **name**. The user must have been previously configured. **name** must be a sequence of characters and/or wildcard characters (‘$’ and ‘*’) from 1 to 127 characters in length. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (’). For example; ‘$’.

**full**

Shows all available subscriber information. The following filter keywords are valid with this command:

- active, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant, fa, fa-service, ggsn-service, ha, ha-service, idle-time, imsi, ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-time-left, msid, network-requested, network-type, pcf, pdsn-service, plmn-type, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

**ggsn-only**

Displays only GGSN-specific subscriber context information.
**gprs-only**

Displays only 2G SGSN subscribers/contexts. The following filter keywords are valid with this command:

aaa-configuration, active, active-charging-service, activity, all, apn, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, full, ggsn-address, gprs-service, gsm-traffic-class, idle-time, imsi, msid, msisdn, partial, plmn-type, rx-data, session-time-left, summary, tx-data, grep, and more.

**gtp-version { 0 | 1 }**

Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1). The following filter keywords are valid with this command:

active-charging-service, apn, bearer-establishment, callid, dhcp-server, fa, fa-service, ggsn-service, gprs-service, gsm-traffic-class, msid, msisdn, plmn-type, ggsn-address, gprs-service, smgr-instance, tx-data, username, grep, more.

**hsgw-only**

Displays HSGW subscriber session information.

The following filters/keywords are valid with this command:

```
    all, full, summary
```

hsgw-service **svc_name**

Displays subscriber information based on the HSGW service name. **svc_name** must be an existing HSGW service and be from 1 to 63 alpha and/or numeric characters.

**hsgw-service svc_name**

Displays subscriber information based on the HSGW service name. **svc_name** must be an existing HSGW service and be from 1 to 63 alpha and/or numeric characters.

**ip-alloc-method { aaa-assigned | dhcp [ relay-agent | proxy-client ] | dynamic-pool | l2tp-1ns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }**

Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:

- **aaa-assigned**: Selects subscribers whose IP Addresses were assigned by AAA.
- **dhcp**: Selects subscribers whose IP Addresses were assigned by DHCP.
  - **relay-agent**: Selects subscribers whose IP Addresses were assigned by the DHCP Relay Agent
  - **proxy-client**: Selects subscribers whose IP Addresses were assigned by the DHCP Proxy Client
- **dynamic-pool**: Selects subscribers whose IP Addresses were assigned from a dynamic IP address pool.
- **l2tp-1ns-assigned**: Selects subscribers whose IP Addresses were assigned by the Layer 2 Tunneling Protocol Network Server.
- **mip-ha-assigned**: Selects subscribers whose IP Addresses were assigned by the Mobile IP Home Agent.
- **ms-provided-static**: Selects subscribers whose IP Addresses were provided by the Mobile Station.
- **not-ms-provided-static**: Selects subscribers whose IP Addresses were not provided by the Mobile Station.
- **static-pool**: Selects subscribers whose IP Addresses were assigned from a static IP address pool.

**ipsg-only**

Displays IPSG subscriber session information.
show subscribers

**lma-service** *svc_name*
Displays subscriber information based on the LMA service name. *svc_name* must be an existing LMA service and be from 1 to 63 alpha and/or numeric characters.

**mag-service** *svc_name*
Displays subscriber information based on the MAG service name. *svc_name* must be an existing MAG service and be from 1 to 63 alpha and/or numeric characters.

**mme-address**
Displays subscriber information based on the MME IP address. *ip_address* must be an existing MME IP address and be entered in IPv4 dotted decimal notation.

**mme-only**
Displays MME subscriber session information.
The following filter keywords are valid with this command:

```
all, full, summary
```

**pdg-only**
Displays a summary of PDG subscriber statistics.

**pdg-service** *name*
Displays statistics for users associated with a specific PDG service name.

**pdif-only**
Displays a summary of PDIF subscriber statistics.

**pdif-service** *name*
Displays connection statistics for users associated with a specific pdif-service name.

**pgw-only**
Displays P-GW subscriber session information.
The following filters/keywords are valid with this command:
**show subscribers**

```
all, full, summary

pgw-service svc_name: Displays subscriber information based on the P-GW service name. svc_name must be an existing P-GW service and be from 1 to 63 alpha and/or numeric characters.
sgw-address ip_address: Displays subscriber information based on the S-GW IP address. ip_address must be an existing S-GW IP address and be entered in IPv4 dotted decimal notation.
```

```
qci number
Displays subscriber session information based on the QCI value assigned to the subscriber. number must be an integer value from 0 to 9.
```

```
slu-state { active | idle | idle-active }
Displays session information based on the subscriber’s S1-U state. The S1-U interface is the interface from the eNodeB to the S-GW.
active: Displays session information for subscribers with an S1-U state set to active.
idle: Displays session information for subscribers with an S1-U state set to idle.
idle-active: Displays session information for subscribers with an S1-U state set to idle-active.
```

```
s5,proto { gtp | pmip }
Displays subscriber session information based on the S5 interface protocol used. Choose either GPRS Tunneling Protocol (GTP) or Proxy Mobile IP (PMIP).
```

```
sgsn-only
Displays only 3G SGSN-specific subscriber context information. The following filters are valid with this command:
aaa-configuration, active, active-charging-service, activity, all, apn, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, full, ggsn-address, gsm-traffic-class, idle-time, imsi, msid, msisdn, partial qos [requested | netogitated ], plmn-type, rnc, rx-data, session-time-left, summary, tx-data, grep, and more.
```

```
sgw-only
Displays S-GW subscriber session information.
The following filters/keywords are valid with this command:

```
all, full, summary

sgw-service svc_name: Displays subscriber information based on the S-GW service name. svc_name must be an existing S-GW service and be from 1 to 63 alpha and/or numeric characters.
pgw-address ip_address: Displays subscriber information based on the P-GW IP address. ip_address must be an existing P-GW IP address and be entered in IPv4 dotted decimal notation.
```

```
sgw-service svc_name
Displays subscriber information based on the S-GW service name. svc_name must be an existing S-GW service and be from 1 to 63 alpha and/or numeric characters.
```

```
subscription { aor address | callid id | full }
Displays subscription information for defined subscribers, based on defined parameters.
aor address: Clear session(s) by Address of Record.
callid id: Specific Call Identification Number.
```
full: Displays all available information.

summary
Only display a summary of the subscriber information. The following filter keywords are valid with this command:
active, activity, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant, enodeb-address, fa, fa-service, ggsn-service, ha, ha-service, idle-time, imsi ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-time-left, msid, network-requested pcf, pdsn-service, plmn-type, rx-data, session-time-left, sgsn-address, tx-data, username, grep, more

tft
Displays the current Traffic Flow Template (TFT) associated with the subscriber session.

tx-data
Bytes transmitted by the subscriber.

wf1
Displays subscriber information in wide format number 1. Wide format number 1 includes the following information for each listed subscriber session:
• Access Type
• Access Technology
• Call State
• Link Status
• Network Type
• Call ID
• MSID
• Username
• IP Address
• Time-Idle
• Access Peer Address
• Service Address
• Network Peer Address
• Connect Time

filter_keywords
The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line. When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.
For example; if you enter the following command:
show subscribers counters ip-pool pool1 card-num 1
show subscribers

Counters for all subscriber sessions that were assigned an IP address from the IP pool named pool1 and also are being processed by the processing card in slot 1 is displayed. Information for all other subscribers is not displayed.

**active**
Only display information for those subscribers who currently have active sessions.

**active-charging-service acs_service**
Displays information for subscribers under active charging service processing. 
*acs_service* must be a string of 1 through 15 characters in length.

**all**
If no keywords are specified before *all*, information for all subscribers is displayed. If keywords are specified before *all*, all information is displayed with no further options being allowed.

**apn name**
Displays subscribers currently facilitated by the Access Point Name (APN) template called *name* configured on the system. This command is for GGSN only.

**asngw-only**
Displays counters for subscribers accessing the ASN GW service only.

**asnpnc-only**
Displays counters for subscribers accessing the ASN Paging Controller and Location Registry service only.

**callid id**
Displays subscriber information for the call specified by *id*. The call ID must be specified as an 8-byte hexadecimal number.

**card-num card_num**
The slot number of the processing card by which the subscriber session is processed. *card_num* is a slot number from 1 through 7 or 10 through 16.

**cocoa-only**
Displays the subscribers that registered a MIP colocated COA directly with the HA. This option is only valid when MIPHA session license is enabled.

**configured-idle-timeout [ < | > | greater-than | less-than ] value**
Shows the idle timeout that is configured for the specified subscriber. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.
*<*: Filters output so that only information less than the specified value is displayed.
*>: Filters output so that only information greater than the specified value is displayed.
*greater-than*: Filters output so that only information greater than the specified value is displayed.
*less-than*: Filters output so that only information less than the specified value is displayed.
*value*: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.
**connected-time** [ < | > | greater-than | less-than ] value

Shows how long the subscriber has been connected. <: Filters output so that only information less than the specified value is displayed. 
>: Filters output so that only information greater than the specified value is displayed. 
greater-than: Filters output so that only information greater than the specified value is displayed. 
less-than: Filters output so that only information less than the specified value is displayed. 
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 4294967295.

**cscf-only**
Displays information for CSCF subscribers only.

**cscf-service service_name**
Displays information for subscribers accessing the specified CSCF service. 
*service_name* must be an existing service and be from 1 to 63 alpha and/or numeric characters in length.

**dhcp-server address**
Displays subscribers currently accessing the system that have been provided an IP address by the DHCP server specified by *address*. This command is for GGSN only.

**dormant**
Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**enodeb-address IPv4_address**
Displays information for EPS subscribers connected to the eNodeB specified by *IPv4_address*. The address must be specified using the standard IPv4 dotted decimal notation.

**fa address**
Displays information for subscribers connected to the foreign agent specified by *address*. The address must be specified using the standard IPv4 dotted decimal notation.

**fa-only**
Only display FA-specific context information.

**fa-service name**
Displays information for subscribers connected to the foreign agent service specified by *name*. The foreign agent service name must have been previously defined.

**firewall { not-required | required }**
Displays information for the specified subscribers: 
not-required: Subscribers for whom firewall processing is not required. 
required: Subscribers for whom firewall processing is required.
**firewall-policy fw_policy_name**
This keyword is obsolete.

**fw-and-nat policy fw_nat_policy**

**Important:** This option is customer-specific and is only available in StarOS 8.1.

Displays information for subscribers using the specified Firewall-and-NAT policy.

*fw_nat_policy* specifies the Firewall-and-NAT policy name, and must be an alpha and/or numeric string of 1 through 15 characters in length.

**ggsn-address ip_address**
Displays information for subscribers connected to the GGSN with specific IP address specified by *ip_address*. The GGSN IP address *ip_address* must have been previously defined.

*ip_address:* must use dotted decimal notation.
This keyword is for SGSN only.

**ggsn-preservation-mode**
Displays information for subscribers connected to the GGSN service with preservation mode enabled. This filter keyword is for GGSN only.

**ggsn-service name**
Displays information for subscribers connected to the GGSN service specified by *name*. The GGSN service *name* must have been previously defined. This keyword is for GGSN only.

**gsm-traffic-class { background | conversational | interactive | streaming }**
Displays information for subscriber traffic that matches the specified 3GPP traffic class.

- **background:** 3GPP QoS background class.
- **conversational:** 3GPP QoS conversational class.
- **interactive:** 3GPP QoS interactive class. Must be followed by a traffic priority.
- **streaming:** 3GPP QoS streaming class.

**ha address**
Displays information for subscribers connected to the home agent specified by *address*. The address must be specified using the standard IPv4 dotted decimal notation.

**ha-ipsec-only**
Only display information for subscriber sessions that are using IP-Security.

**ha-only**
Only display HA-specific context information.
ha-service name
Displays information for subscribers connected to the home agent service specified by name. The home agent service name must have been previously defined.

idle-time [ < | > | greater-than | less-than ] value
Displays how long the subscriber session has been idle or display subscriber sessions that meet the idle time criteria specified.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 4294967295.

ims-auth-service service_name
Displays information for subscribers with specified IMS Authorization Service. service_name must have been previously defined.

imsi id
Shows the subscriber with the specified id. The IMSI (International Mobile Subscriber Identity) ID is a 15 character field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (’). For example; ‘$’.

ip-address [ < | > | greater-than | less-than ] address
Displays information for subscribers connected to the specified address.
<: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
>: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
greater-than: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
less-than: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
address: The address must be specified using the standard IPv4 dotted decimal notation. Used in conjunction with <, >, greater-than, less-than. If the ip address is specified without a qualifier then only subscribers with the specified IP address have their information displayed.

ip-pool name
Displays information for subscribers assigned addresses from the IP address pool name. name must be the name of an existing IP pool or IP pool group. IP pool name will be either ipv4 or ipv6 according to call line setup for specified pool name.

ipv6-address address
Displays information for subscribers connected to the specified address.
**ipv6-prefix prefix**
Displays information for subscribers connected to the specified address and `prefix`.

**lac address**
Displays information for calls to the peer LAC (L2TP access concentrator) specified by `address`.

**lac-only**
Show L2TP LAC specific information only.

**lac-service name [ local-tunnel-id id | remote-tunnel-id id ]**
Displays information for calls associated with the LAC service named `name`. This is a string of 1 to 63 characters.
- `local-tunnel-id id`: Specifies a specific local tunnel from which to clear calls. `id` must be in the range of 1 to 65535.
- `remote-tunnel-id id`: Specifies a specific remote tunnel from which to clear calls. `id` must be in the range of 1 to 65535.

**13-tunnel-local-addr ip_address**
Specific layer 3 tunneling interface specified by `ip_address`. The address must be specified using the standard IPv4 dotted decimal notation.

**13-tunnel-remote-addr ip_address**
Specific layer 3 tunneling peer specified by `ip_address`. The address must be specified using the standard IPv4 dotted decimal notation.

**lns address**
Displays information for calls to the peer LNS (L2TP network server) specified by `address`.

**lns-only**
Show L2TP LNS specific information only.

**lns-service name [ local-tunnel-id id | remote-tunnel-id id ]**
Displays information for calls associated with the LNS service named `name`. This is a string of 1 to 63 characters.
- `local-tunnel-id id`: Specifies a specific local tunnel from which to clear calls. `id` must be in the range of 1 to 65535.
- `remote-tunnel-id id`: Specifies a specific remote tunnel from which to clear calls. `id` must be in the range of 1 to 65535.

**long-duration-time-left [ < | > | greater-than | less-than ] value**
Shows how much time is left for the maximum duration of a specified subscriber session.
- `<`: Filters output so that only information less than the specified value is displayed.
- `>`: Filters output so that only information greater than the specified value is displayed.
- `greater-than`: Filters output so that only information greater than the specified value is displayed.
- `less-than`: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 4294967295.

mip-udp-tunnel-only
Displays the subscribers that negotiated MIP-UDP tunneling with the HA. This option is only valid when MIP NAT Traversal license is enabled.

mipv6ha-only
Shows MIPV6HA-specific context information for the session.

mipv6ha-service service_name
Displays specific configured MIPV6 Home Agent service. service_name must have been previously defined.

msid id
Displays information for the mobile user identified by id. id must be from 7 to 16 hexadecimal digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘’). For example: ‘$’.

In case of enforce imsi-min equivalence is enabled on the chasis and MIN or IMSI numbers supplied, this filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.

show subscribers msid ABCD0123456789 or
show subscribers msid 0123456789
will show any subscriber with a MSID that match the lower 10 digits of MSID supplid, i.e. 0123456789.

msisdn msisdn
Displays information for the mobile user identified by the Mobile Subscriber ISDN Number (MSISDN). msisdn must be 7 to 16 digits; specified as an IMSI, MIN, or RMI.

nat { not-required | required [ nat-ip nat_ip_address | nat.realm nat.realm ] }
Displays information for the specified subscribers.
not-required: Subscribers for whom Network Address Translation (NAT) processing is not required.
required: Subscribers for whom NAT processing is required.

Important: The nat-ip keyword is only available in StarOS 8.3 and later.

nat-ip nat_ip_address: Subscribers for whom NAT processing is enabled and are using the specified NAT IP address. nat_ip_address specifies the NAT IP address and must be a standard IPv4 address.
nat.realm nat.realm: Subscribers for whom NAT processing is enabled and are using the specified NAT realm. nat.realm specifies the NAT realm name and must be a string from 1 through 63 characters in length.
show subscribers

network-requested
Display information for currently active subscribers whose sessions were initiated by the GGSN network requested create PDP context procedure.

network-type { gre | ipip | ipsec | ipv4 | ipv6 | l2tp | mobile-ip | proxy-mobile-ip }
Displays network type information for the subscriber session. The following network types can be selected:
* gre: Generic Routing Encapsulation (GRE) per RFC 2784
* ipip: IP-in-IP encapsulation per RFC 2003
* ipsec: IPSec
* ipv4: Internet Protocol version 4 (IPv4)
* ipv6: Internet Protocol version 6 (IPv6)
* l2tp: Layer 2 Tunneling Protocol encryption per RFC 2661
* mobile-ip: Mobile IP
* proxy-mobile-ip: Proxy Mobile IP

nsapi nsap_id
Displays session information for the mobile user identified by network service access point identifier (NSAPI) between MS and SGSN. NSAPI is also used as part of the Tunnel Identifier between GPRS Support Nodes (GSNs). The user identity IMSI and the application identifier (NSAPI) are integrated into the Tunnel Identifier (GTPv0) (TID) or Tunnel Endpoint Identifier (GTPv1) (TEID) that uniquely identifies the subscriber’s sublink between the GSNs (SGSN and GGSN). The NSAPI is an integer value within the PDP context header.
nsap_id must be an integer value from 5 through 15.

partial qos { negotiated | requested }
This filter is specific to the SGSN.
Is limits the display of information to requested or negotiated QoS information for the subscriber.
This filter can be used in combination with further defining filters: active, active-charging-service, all, apn, callid, card-num, configured-idle-timeout, connected-time, ggsn-address, gprs-service, gsm-traffic-class, idle-time, imsi, msid, misisd, negotiated, plmn-type, requested, rx-data, session-time-left, tx-data

pcf [ < | > | less-than | greater-than ] ipv4_address [ [ < | > | less-than | greater-than ] ipv4_address ]
Displays information for subscribers connected via the packet control function with a specific or range of IP address ipv4_address. The address must be specified using the standard IPv4 dotted decimal notation.
* <: Filters output so that only information less than the specified IPv4 address value is displayed.
* >: Filters output so that only information greater than the specified IPv4 address value is displayed.
* less-than: Filters output so that only information less than the specified IPv4 address value is displayed.
* greater-than: Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.
show subscribers

**pdsn-only**
Show PDSN specific information only.

**pdsn-service name**
Displays information for subscribers connected to the packet data service *name*. The packet data service must have been previously configured.

**plmn-type**
Displays subscriber type (HOME, VISITING, or ROAMING). This keyword is for the GGSN or the SGSN only.

**policy**
Displays the current policies associated with the subscriber session.

**rnc id rnc_id mcc mcc_num mnc mnc_num**
Displays information for subscribers connected to the SGSN via a specific RNC (radio network controller) identified by the RNC ID, the MCC (mobile country code), and the MNC (mobile network code). This keyword is for SGSN only.

**rx-data [< | > | greater-than | less-than ] value**
The number of bytes received by the specified subscriber.
- `<`: Filters output so that only information less than the specified value is displayed.
- `>`: Filters output so that only information greater than the specified value is displayed.
- `greater-than`: Filters output so that only information greater than the specified value is displayed.
- `less-than`: Filters output so that only information less than the specified value is displayed.

**session-time-left [< | > | greater-than | less-than ] value**
How much session time is left for the specified subscriber.
- `<`: Filters output so that only information less than the specified value is displayed.
- `>`: Filters output so that only information greater than the specified value is displayed.
- `greater-than`: Filters output so that only information greater than the specified value is displayed.
- `less-than`: Filters output so that only information less than the specified value is displayed.

**smgr-instance number**
Specific sessmgr instance. *number* must be in the range of 1 to 4294967295.

**sgsn-address address**
Shows information for subscribers whose PDP contexts are currently being facilitated by the SGSN specified by address. This command is for GGSN only.
shows subscribers

sgsn-service srvc_name
Shows subscriber information for a specified 3G SGSN service.
srvc_name must be a string of 1 to 63 alphanumeric characters that identifies a configured SGSN service. This command is for SGSN only.

tx-data [ < | > | greater-than | less-than ] value
The number of bytes transmitted by the specified subscriber.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 18446744073709551615.

username name
Displays information for connections for the subscriber identified by name. The user must have been previously configured. name must be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters in length. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

verbose
Display detailed information.

grep grep_options | more
Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view information about subscriber sessions.
The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant subscribers.
The Command Keywords may be used standalone to display detailed information or you may use one or more of the various Filter Keywords to reduce the amount of information displayed.

⚠️ Caution: Executing this command may negatively impact performance if multiple instances are executed while the system is under heavy load and simultaneously facilitating multiple CLI sessions.

Example
The following command displays information for all subscriber sessions:

show subscribers all
The following command displays information for all ggsn-only subscriber sessions:

```
show subscribers ggsn-only all
```

The following command displays information for all subscriber sessions in wide format 1:

```
show subscribers w1 all
show subscribers aaa-configuration
show subscribers counters username ispluser1
```

The following command displays information for subscriber in GGSN service:

```
show subscribers ggsn-only all
show subscribers ggsn-only full
```

The following command displays information for all subscriber with SGSN session having partial QoS requests:

```
show subscribers sgsn-only partial qos requested
```

The following command displays information for all subscriber with MME session connected to MME service having IP address as 1.1.1.1:

```
show subscribers mme-only mme-address 1.1.1.1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show super-charger

Lists subscribers with valid super charger configuration.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show super-charger { imsi imsi | all }
```

- **imsi**
  Defines a specific subscriber’s international mobile subscriber identity (IMSI) number.
  **imsi** - up to 15 digits This number includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number),

- **all**
  Instructs the SGSN to display super charger subscription information for all subscribers.

Usage
Use this command to determine if a single subscriber, identified by the IMSI, has a super charger configuration. Also, this command can display the list of all subscribers with a super charger configuration. If a subscriber has super charger as part of the configuration, then subscriber data is backed up (using the IMSI Manager) after the subscriber detaches and the purge timer expires.

Example
The following command displays the super charger configuration information for the subscriber identified by the IMSI 90121882144672.

```
show super-charger imsi 90121882144672
```
show support details

This command outputs a comprehensive list of system information that is useful for troubleshooting purposes. In most cases, the output of this command is requested by the technical support team.

Product
All

Privilege
All

Syntax

```
show support details [ to file url]
```

to file url

Specifies the location where a tar file with the support detail information should be created. url may refer to a local or a remote file. url must be entered using one of the following formats:

- ASR 5000:
  ```
  ![file:]{/flash|/pcmcia|/hd}[/{directory}]/{file_name}
  ![tftp:]{host[:port]}[/{directory}]/{file_name}
  ![ftp: | sftp: ]/{username}:{password}@{host}:{port}]
  ![directory]/{file_name}
  ```

- filename is the directory name.
- username is the user to be authenticated.
- password is the password to use for authentication.
- host is the IP address or host name of the server.
- port# is the logical port number that the communication protocol is to use.

If the filename is not specified with a .tar extension, it is automatically appended to the filename when the file is created and a message is generated.

The content of the tar file is as follows:

- **support_summary** - An ASCII text file that contains the support detail information.
- **information.minicores.tar** - A tar file that contains any minicore files found on the system. Minicore files contain memory core dumps that are captured during some events. These core dumps provide specific memory locations and other information about the event. This information is useful to the technical support team in identifying specifically where an event occurred and its probable cause.

Usage

Use this command to obtain extensive system information for use in troubleshooting. This command does the work of over 30 separate commands, which saves time and ensures that all of the information needed is collected and displayed in the same order every time. The output of the following commands is included:

- show version verbose
- show config
- show context
- show ip pool
- show ip interface
- show ip route
- show boot
- show boot initial-config
- show system uptime
- show license information
- show card hardware
- show card info
- show card diag
- show card table all
- show port table all
- show port info
- show port npu counters
- show port datalink counters
- show fans
- show hardware version fans
- show power chassis
- show alarm audible
- show alarm central-office
- show alarm outstanding
- show alarm statistics
- show asngw-service statistics
- show asnpe-service statistics
- show content-filtering category database
- show cpu table
- show cpu info verbose
- show resources
- show task table
- show task resources
- show task resources max
- show crash list
- show snmp trap history
- show logs level error
- show logs level error inactive
- show ppp statistics
- show session disconnect-reasons
- show apn statistics all
• show pdsn-service all
• show ha-service all
• show dhcp-service all
• show ggsn-service all
• show lac-service all
• show lns-service all
• mme-hss-service
• mme-service
• show session progress
• show rp statistics
• show mipfa statistics
• show mipha statistics
• show srp info
• show srp checkpoint statistics
• show srp checkpoint statistics verbose
• show gtpc statistics verbose
• show gtp accounting servers
• show gtpp statistics verbose
• show gtpp storage-server
• show session recovery status verbose
• show clock all
• show radius counters all
• show ntp associations all
• show charging-service all (if the Enhanced Charging Service license is installed)
• show qos npu inter-subscriber traffic bandwidth-sharing
• timestamps
• no timestamps

In addition to the information provided by the above commands, the show support details command includes information that is not otherwise accessible to users but that is helpful in the swift resolution of issues.

Example
The following command displays the system information on your console.

    show support details

The following command displays the information on your console and also writes it to the local device (pcmcia1 in this case) and includes the mini core dumps, using the filename r-p_problem.tar.

    show support details to file /pcmcia1/r-p_problem.tar
The following command displays the information on your console and also writes it to an FTP server (named host), placing the file in the dir directory and includes the mini core dumps, using the filename re_problem.tar.

```
show support details to file ftp://host/dir/re_problem.tar
```
show system uptime

Shows the system the amount of time the system has been operational since the down time (maintenance or otherwise).

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show system uptime [ | { grep grep_options | more } ]
```

| **uptime** |
| Indicates only the system up time is to be displayed. |

| **grep grep_options | more** |
| Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference. |

**Usage**
Display the system up time to check for the possibility of anomalous behavior related to longer up times.

**Example**
The following commands display the system basic information and up time only, respectively.

```
show system uptime
```
Chapter 97
Exec Mode Show Commands (T-Z)

This section includes the commands `show task` through `show version`
show task

Displays information about system tasks.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show task { info | resources | table } [ card card_num ] [ facility facility { all | instance id } ] [ process process_name { all | max } ] [ grep grep_options ]
```

- **{ info | resources | table }**
  Specifies type of information to be displayed and scope of tasks to include in output.
  - `info`: Display detailed task information.
  - `resources`: Display resource allocation and usage information for all tasks.
  - `table`: Display identification information in tabular format for all tasks.

- **card card_num**
  Default: all powered on cards.
  Specifies a single card for which task information is to be displayed where `card_num` must be from 1 to 48.

- **facility facility { all | instance id }**
  Default: all facilities.
  Specifies the list of facilities for which task information may be displayed. A specific instance of the facility may be displayed as specified by `id` or all instances may be displayed. The value of `id` must be in the range of 0 through 100000. `facility` must be one of:
  - `allmgr`: A11 Interface Manager facility
  - `aaamgr`: AAA Manager Facility
  - `aaaproxy`: AAA Proxy manager Facility
  - `acscctrl`: Active Charging Service (ACS) Controller Facility
  - `acsmgr`: Active Charging Service (ACS) Manager Facility
  - `asngwmg`: ASN Gateway Manager
  - `asnpcrm`: ASN Paging/Location-Registry (ASN-PC) Manager
  - `bgp`: Border Gateway Protocol (BGP) Facility
  - `bulkstat`: Bulk Statistics Manager Facility
  - `cdrmod`: Charging Detail Record Module
  - `cli`: Command Line Interface Facility
  - `cscfmg`: SIP CSCF Manager
  - `csctrl`: Card Slot Port controller Facility
• **cssctrl**: Content Service Steering Controller  
• **dcardctrl**: IPSEC Daughtercard Controller Logging Facility  
• **dcardmgr**: IPSEC Daughtercard Manager Logging Facility  
• **dhmgr**: Distributed Host Manager  
• **drvctrl**: Driver Controller Facility  
• **egtpemgr**: EGTP Egress Demux Manager  
• **egtpinmgr**: EGTP Ingress Demux Manager  
• **evlogd**: Event Log Daemon Facility  
• **famgr**: Foreign Agent Manager Facility  
• **gtpcmr**: GTP-C Protocol Logging facility (GGSN product only)  
• **h248pmt**: H.248 Protocol Task  
• **hamgr**: Home Agent Manager Facility  
• **hatcpu**: High Availability Task CPU Facility  
• **hatsystem**: High Availability Task Facility  
• **ipsecctrl**: IP Security Controller Facility  
• **ipsecemgr**: IP Security Manager Facility  
• **ipsmgmr**: IP Services Gateway Facility  
• **l2pdemux**: L2TP Demultiplexor (LNS) Facility  
• **l2pemgr**: L2TP Manager Facility  
• **magmgr**: Mobile Access Gateway Manager  
• **megadiammgr**: MegaDiameter Manager  
• **mmedemux**: MME Demux Manager logging facility  
• **mmemgr**: MME Manager logging facility  
• **mmgr**: SGSN/SS7 Master Manager  
• **mttest**: Migration Performance Test on Packet Accelerator Card  
• **netwstrg**: Network Storage Manager  
• **npuctrl**: Network Processor Unit control Facility  
• **npumgr**: Network Processor Unit Manager Facility  
• **nputst**: Network Processor Unit Tester  
• **nsctrl**: Charging Service Controller  
• **nsmgr**: Charging Service Process Manager  
• **orbs**: Object Request Broker Notification Server Facility  
• **orbs**: Object Request Broker System Facility  
• **ospf**: Open Shortest Path First Facility  
• **rct**: Recovery Control Task Facility  
• **rdt**: Redirect Task Facility  
• **rip**: Routing Information Protocol Facility
show task

- **rmctrl**: Resource Manager Controller Facility
- **rmmgr**: Resource Manager Facility
- **sct**: Shared Configuration Task Facility
- **sessctrl**: Session Controller Facility
- **sessmgr**: Session Manager Facility
- **sft**: Switch Fabric Monitoring Task
- **sipcdprt**: Sip Call Distributor Task
- **sitmain**: System Initialization Task Main Facility
- **sitparent**: Card based system initialization facility that applies to Packet Accelerator Cards and Switch Processor Cards

**Important**: **sitparent** replaces the facilities **sitpac**, **sitspc** and **sittac**.

- **snmp**: SNMP Protocol Facility
- **srdb**: Static Rating Database
- **threshold**: Threshold Server Facility
- **vpncntl**: Virtual Private Network Controller Facility
- **vpnmgr**: VPN Manager Facility
- **zebos**: ZEBOS™ OSPF Message Facility

**all**: Display information for all instances of the specified facility.
**instance id**: Display information for the specified instance of the specified facility only. id must be an integer from 0 through 10000000.

**process process_name all**

Display information for all instances of the specified process. must be one of the following process names:
- **ftpd**: File Transfer Protocol Daemon
- **inetd**: Internet Super-server Daemon
- **nsproc**: NetSpira Packet Processor
- **ntpd**: Network Time Protocol Daemon
- **orbsnd**: Object Request Broker Notification Server
- **ping**: Ping
- **pvmd-wrapper**: NetSpira Messenger Daemon
- **pvmgs**: NetSpira Messenger Daemon
- **rlogin**: Remote Login
- **sftp-server**: Secure File Transfer Protocol Server
- **sitreap**: System Initialization Task Cleanup Process
- **sn_resolve**: DNS Resolver Process
- **ssh**: Secure Shell
- **sshd**: Secure Shell Daemon
Exec Mode Show Commands (T-Z)

**show task**

- **telnet**: Telnet
- **telnetd**: Telnet Daemon
- **tftpd**: Trivial File Transfer Protocol Daemon
- **traceroute**: Traceroute

### max

Default: current usage levels are displayed.
Displayed the maximum usage levels for tasks as opposed to the current usage levels.
The keyword **max** is valid only in conjunction with the **resources** keyword.

### grep grep_options | more

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

### Usage

Display task information as part of system troubleshooting unexpected behavior.

### Important: This command is not supported on all platforms.

### Example

The following commands provide some examples of the combinations of options that may be used to display task information.

```plaintext
show task info facility hatspc all
show task info facility hatspc instance 456
show task resources facility zebos all
show task table facility ospf
show task table card 8 facility cli all
show task resources facility rip all max
```
**show temperature**

Displays the current temperature on all installed application and line cards. Also displays the temperature of upper and lower fan trays. Temperature readings are acquired from sensors located on these components.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show temperature [ verbose] [ | { grep grep_options | more } ]
```

- **grep grep_options | more**
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

- **verbose**
  Indicates that the output is to contain detailed information.

**Usage**

Verify current temperature of components in chassis.

**Example**

```
show temperature
show temperature verbose
```
show terminal

Displays the current terminal settings for number of lines in length and number of characters in width.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show terminal [ | { grep grep_options | more } ]
```

```
grep grep_options | more
```

Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage

Verify current terminal settings in case the output displayed appears to have line breaks/wraps in unexpected places.

Example

```
show terminal
```
show threshold

Displays thresholding information for the system.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show threshold [ default ]
```

[ default ]
Used to display the system’s thresholding default values.

**Usage**
Use this command to display information on threshold value configuration and activity.

**Example**
The following command displays configuration information pertaining to threshold values configured on the system:

```
show threshold
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show timing

Displays the information configured to define a transmit timing source other than the system clock. The display includes related information (such as port status, timing source priority, timing alarms, etc.) for all of the ports configured for either BITS or line timing.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show timing
```

**Usage**

Use this command to determine which line cards are recovering receive timing clocks.

**Important:** This command is not supported on all platforms.

**Example**

The following command displays timing configuration and status information for the timing-configured ports.

```
show timing
```
show upgrade

Displays the status of an on-going on-line software upgrade.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show upgrade
```

**Usage**
Use this command to show the status of an on-going on-line software upgrade.

**Important:** This command is not supported on all platforms.
show url-blacklisting database

This command displays URL Blacklisting static database configurations.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show url-blacklisting database [ all | url url | facility acsmgr { all | instance instance } ] [ | { grep grep_options | more } ]
```

- **all**
  Displays configurations of all URL Blacklisting databases present in the default or override directory.

- **facility acsmgr { all | instance instance }**
  Displays configurations of URL Blacklisting database configuration per facility/ACSMgr instance.
  - **all**: Displays URL Blacklisting database configuration of all ACSMgrs.
  - **instance instance**: Displays URL Blacklisting database configuration of the specified instance.
    - `instance` must be instance number of the database, and must be an integer from 1 through 1000000.

- **url url**
  Displays configurations of the URL Blacklisting database specified in the URL.
  - `url` must be the database's URL, and must be a string of 1 through 512 characters in length.

- **grep grep_options | more**
  Specifies that output of this command is to be piped (sent) to the command specified. A command to send the output to must be specified.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view configurations associated with in-memory and on-flash Blacklisting database. The `show url-blacklisting database` command displays the active database that is loaded, and is the one set by either the default or override CLI commands.

Example

The following command displays configurations of all the databases present in default or override directory, indicating one as ACTIVE and rest as NOT LOADED:

```
show url-blacklisting database all
```

The following command displays configurations of the `/flash/bl/optblk.bin` database:
The following command displays database configuration for the ACSMgr instance 1:

```
show url-blacklisting database facility acsmgr instance 1
```
show version

Displays the version information for the current system image or for a remote image.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show version [ url ] [ all | verbose ] [ | { grep | grep_options | more } ]
```

- **url**
  Specifies the location of a configuration file to display version information for. The `url` may refer to a local or a remote file. `url` must be entered using one of the following formats:
  - **ASR 5000:**
    - `{ file: }[/flash|/pcmcia|/hd ][/directory]/file_name`
    - `tftp://host[:port#][/directory]/file_name`
    - `http: | ftp: | sftp: ]//username[:password]@host[:port#][/directory]/file_name`

  - `directory` is the directory name.
  - `filename` is the actual file of interest.
  - `username` is the user to be authenticated.
  - `password` is the password to use for authentication.
  - `host` is the IP address or host name of the server.
  - `port#` is the logical port number that the communication protocol is to use.

- **all | verbose**
  - `all`: indicates all image information is to be displayed.
  - `verbose`: indicates the output is to contain detailed information.

  The `verbose` keyword may not be used in conjunction with a URL specification.

- **grep | grep_options | more**

  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Cisco ASR 500 Series Command Line Interface Reference.

Usage

Display the version information to verify the image versions loaded in preparation for maintenance, upgrades, etc.

**Important:** This command is not supported on all platforms.
Example
The following commands display the version information with the basic level of output and the detailed level, respectively.

    show version
    show version verbose
Chapter 98
FA Service Configuration Mode Commands

The Foreign Agent Service Configuration Mode is used to create and manage the Foreign Agent (FA) services associated with the current context.

```
Exec Mode
configure
Global Configuration Mode
context name
Context Configuration Mode
fa-service name
FA Service Configuration Mode
```
advertise

Configures agent advertisement parameters within the FA service.

**Product**
PDSN, GGSN, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
advertise {adv-delay seconds | adv-lifetime time | adv-interval { seconds | msec num } | num-adv-sent number | prefix-length-extn | reg-lifetime reg_time}
```

```
noadvertise {prefix-length-extn | reg-lifetime}
```

[default] advertise adv-delay

```
no advertise prefix-length-extn
```

Disables prefix-length-extn

```
no advertise reg-lifetime
```

Specifies that there is no limit to the registration lifetime that the FA service will allow in any Registration Request message from the mobile node.

```
default advertise adv-delay
```

Sets the initial delay for the unsolicited advertisement to default value of 1000 ms.

```
advertise adv-delay seconds
```

Default: 1000
This command sets the initial delay for the unsolicited advertisement.

`seconds` is the advertisement delay in milliseconds and must be an integer from 10 through 5000.

**Important:** This command is available for WiMAX CMIP calls only.

```
adv-lifetime time
```

Default: 9000
Specifies the FA agent advertisement lifetime.
The agent advertisement lifetime is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements.
time is measured in seconds and can be configured to any integer value between 1 and 65535.

```
adv-interval { seconds | msec num }
```

Default: 5 seconds
Specifies the amount of time between agent advertisements.
seconds is the time in seconds and can be any integer value from 1 through 1800.
**msec num** Configures agent advertisement interval in milliseconds. can be any integer from 100 through 1800000.

**num-adv-sent number**
Default: 5
Specifies the number of unanswered agent advertisements that the FA service sends upon PPP establishment before it will reject the session. number can be any integer value between 1 and 65535.

**prefix-length-extn**
Default: Disabled
When this is enabled, the FA includes the FA-service address in the Router Address field of the Agent Advertisement and appends a Prefix Length Extension in Agent Advertisements with a prefix length of 32.

**reg-lifetime reg_time**
Default: 600
Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. reg_time is measured in seconds and can be configured to any integer value between 1 and 65534.

**Usage**
Use to tailor FA advertisements to meet your network needs and/or conditions.

**Example**
The following command configures the FA advertisement interval at 10 seconds, the advertise lifetime to 20000 seconds, and the maximum number of unanswered advertisements that will be sent to 3.

```
advertise adv-interval 10 adv-lifetime 20000 num-adv-sent 3
```
authentication aaa

This configuration enables/disables the authentication parameters for the FA service to override dynamic keys from AAA with static keys to support MIP registration with HA which do not support dynamic keys.

Product
FA, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

[ no | default ] authentication aaa-distributed-mip-keys override

no
Disable the override of dynamic keys from AAA.

default
By default the override behavior is disabled and system uses dynamic keys from AAA after successful EAP authentication. When no EAP authentication happens system uses static keys by default.

Usage
Specify how the system will perform authentication of registration request messages. By default dynamic MN-HA and FA-HA keys from AAA after successful EAP authentication used by PMIP client in WiMAX calls for MIP registration with HA. This configuration in FA service overrides the dynamic keys from AAA with static keys to support MIP registration with HA which do not support dynamic keys.

Example
The following command configures the FA service to override use of AAA MIP keys and force the use of statically configured FA-HA SPI/key for WiMAX calls.

    authentication aaa-distributed-mip-keys override
authentication mn-aaa

Specifies how the system handles authentication for mobile node re-registrations.

**Product**
PDSN, ASN GW, GGS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
```

---

**always**
Specifies that the FA service performs authentication each time a mobile node registers. This is the default setting.

**ignore-after-handoff**
MN-AAA authentication is not done at the FA, for a handoff Access Gateway (AGW).

**init-reg**
MN-AAA and MN-FAC extensions are required only in initialization RRQ.

**init-reg-except-handoff**
MN-AAA and MN-FAC extensions are not required in initialization RRQ after inter-Access Gateway (AGW) handoff.

**renew-and-dereg-noauth**
Specifies that the FA service does not perform authentication for mobile node re-registration or deregistration authorization requests. Initial registration is handled normally.

**renew-reg-noauth**
Specifies that the FA service does not perform authentication for mobile node re-registrations. Initial registration and de-registration are handled normally.

**optimize-retries**
Optimizes the number of Authentication retries sent to the AAA server. When an authentication request is pending for a MIP call at the AGW, if a retry RRQ is received from the mobile node, the AGW discards the old RRQ and keeps the most recent RRQ. Subsequently when the authentication succeeds, the AGW forwards the most recent RRQ to the HA. If the authentication fails, the AGW replies to the MN using the most recent RRQ.

**Usage**
Use this command to determine how the FA service handles mobile node re-registrations. The system is shipped from the factory with the mobile AAA authentication set to always.

**Example**

The following command configures the FA service to perform mobile node authentication for every re-registration:

```
authentication mn-aaa always
```

The following command specifies that the FA service does not perform authentication for mobile node re-registrations:

```
authentication mn-aaa renew-reg-noauth
```
authentication mn-ha

Configures whether the FA service looks for MN-HA auth extension in the RRP.

Product
PDSN, ASN GW, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
authentication mn-ha { allow-noauth | always }
```

---

**allow-noauth**

Allows a reply that does not contain the auth extension.

---

**always**

A reply should always contain the auth extension to be accepted.
This is the default setting.

---

Usage
Use this command to determine whether or not the FA service requires the MN-HA auth extension in the RRP.
The system is shipped from the factory with this set to always.

---

Example
The following command configures the FA service to require a reply to contain the authentication extension to be accepted:

```
authentication mn-ha always
```
bind

Binds the FA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

Product
PDSN, ASN GW, GGSN PDIF

Privilege
Security Administrator, Administrator

Syntax

\[ \text{bind address address [ max-subscribers count ]} \]
\[ \text{no bind address} \]

\[ address \]
Specifies the IP address (address) of the interface configured as the Pi interface. address is specified in dotted decimal notation.

\[ \text{max-subscribers max#} \]
Default: 500000
Specifies the maximum number of subscribers that can access this service on this interface.
\[ \text{count} \]
can be configured to any integer value between 0 and 500000.

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active PACs/PSCs installed in the system. A fully loaded system with 13 active PACs/PSCs can support 500,000 total subscribers. Refer to the license key command for additional information.

Usage
Associate or tie the FA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the max-subscribers option, be sure to consider the following:
- The total number of interfaces you will configure for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to
Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.
Use the no bind address command to delete a previously configured binding.
Example
The following command would bind the logical IP interface with the address of 192.168.3.1 to the FA service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

    bind address 192.168.3.1 max-subscribers 600

The following command disables a binding that was previously configured:

    no bind address
challenge-window

Defines the number of recently sent challenge values that are considered valid by the FA.

**Product**
PDSN, ASN GW, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
challenge-window number
```

- **number**
  - Default: 2
  - The number of recently sent challenge values that are considered valid. `number` must be an integer from 1 through 5.

**Usage**

Use this command to set the number of recently sent challenge values that are considered valid by the FA.

**Example**

Set the challenge window to 3:

```
challenge-window 3
```
**default**

Restores default values assigned for specified parameter.

**Product**
PDSN, ASN GW, GGSN PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
```

<table>
<thead>
<tr>
<th><strong>adv-interval</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Restores the FA advertisement interval to the default value: 5 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>adv-lifetime</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Restores the FA advertisement lifetime to the default value: 9000 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>advertise prefix-length-extn</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the FA from including the FA-service address in the Router Address field of the Agent Advertisement and appending a Prefix Length Extension in Agent Advertisements with a prefix length of 32.</td>
</tr>
</tbody>
</table>

| **authentication { mn-aaa | mn-ha }** |
|-------------------------------------|
| mn-aaa: Restores the FA mobile node registration authentication to the default setting: always. |
| mn-ha: Restores the default setting that an RRP must always contain the MN-HA auth extension to be accepted. |

<table>
<thead>
<tr>
<th><strong>challenge-window</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the number of recently sent challenge values that are considered valid by the FA to the default value of 2.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>dynamic-mip-key-update</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The FA service rejects MIP_Key_Update_Request from the AAA server, not allowing dynamic MIP key updating to occur and terminates the call.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>encapsulation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets Mobile IP (MIP) data encapsulation using GRE to its default: enabled.</td>
</tr>
<tr>
<td>Command</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>`grep { checksum</td>
</tr>
<tr>
<td><code>checksum</code></td>
</tr>
<tr>
<td><code>checksum-verify</code></td>
</tr>
<tr>
<td><code>reorder-timeout</code></td>
</tr>
<tr>
<td><code>sequence-mode</code></td>
</tr>
<tr>
<td><code>sequence-numbers</code></td>
</tr>
<tr>
<td><code>idle-timeout-mode</code></td>
</tr>
<tr>
<td><code>ignore-mip-key-data</code></td>
</tr>
<tr>
<td><code>ignore-stale-challenge</code></td>
</tr>
<tr>
<td><code>ip local-port</code></td>
</tr>
<tr>
<td><code>max-challenge-len</code></td>
</tr>
<tr>
<td><code>mn-aaa-removal-indication</code></td>
</tr>
<tr>
<td><code>multiple-reg</code></td>
</tr>
<tr>
<td><code>num-adv-sent</code></td>
</tr>
<tr>
<td><code>reg-lifetime</code></td>
</tr>
<tr>
<td><code>reg-timeout</code></td>
</tr>
<tr>
<td><code>reverse-tunnel</code></td>
</tr>
</tbody>
</table>
revocation [ enable | max-retransmission | retransmission-timeout | trigger internal-failure ]

Sets the MIP Registration Revocation settings to their default values. When no optional keywords are specified all revocation settings are set to their defaults.

- **enable**: Disables MIP Registration Revocation on the FA.
- **max-retransmission**: Sets the maximum number of retransmissions to 3.
- **retransmission-timeout**: Sets the retransmission timeout to 3 seconds.
- **trigger internal-failure**: Disables the FA from sending revocation messages when a session experiences an internal failure.

**Usage**

After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

**Example**

The following command is used to return the ip local-port parameter to it’s default value:

```
default ip local-port
```
default subscriber

Specifies the name of a subscriber profile configured within the same context as the FA service from which to base the handling of all other subscriber sessions handled by the FA service.

Product
PDSN, ASN GW, GGSN PDIF

Privilege
Security Administrator, Administrator

Syntax

```plaintext
default subscriber profile_name

no default subscriber profile_name
```

profile_name
Specifies the name of the configured subscriber profile. `profile_name` can be between 1 and 63 alpha and/or number characters and is case sensitive.

Usage
Each subscriber profile specifies “rules” such as permissions, PPP settings, and timeout values.
By default, the FA service will use the information configured for the subscriber named default within the same context. This command allows for multiple FA services within the same context to apply different “rules” to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.
Use the `no default subscriber profile_name` command to delete the configured default subscriber.

Example
To configure the FA service to apply the rules configured for a subscriber named user1 to every other subscriber session it processes, enter the following command:

```
default subscriber user1
```
**dynamic-ha-assignment**

This command configures various dynamic HA assignment parameters.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] dynamic-ha-assignment [ aaa-override mn-supplied-ha-addr | allow-failover ]
```

- **default**
  Feature is disabled by default.

- **no**
  Removes the feature and returns it to the default setting of disabled.

- **aaa-override mn-supplied-ha-addr**
  Enables the system to override the mobile node supplied HA IP address with the AAA provided HA address.

- **allow-failover**
  Enables/disables a failover retry for dynamic HA assignment from the AAA server.

**Usage**

Use this command to override the mobile node supplied HA IP address with the AAA supplied HA address. Use this command to enable or disable the failover feature that allows the system to receive and use a newer HA address from the AAA server in cases where the original HA address is not responding. A AAA server may assign different HA addresses each time a retransmitted MIP RRQ is authenticated during the MIP session setup. When this configuration is enabled, if the FA gets a new HA address from AAA during setup, it discards the previous HA address and start using the new address. This allows the FA session to connect to an available HA during setup.

**Example**

The following command enables the failover feature that allows the system to receive and use a newer HA address from the AAA server:

```
dynamic-ha-assignment allow-failover
```
**dynamic-mip-key-update**

When enabled, the FA service processes MIP Key_Update_Request from the AAA server and allows dynamic MIP key updates (DMUs).

Default: Disabled

**Product**
PDSN, ASN GW, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
dynamic-mip-key-update
no dynamic-mip-key-update
```

**Example**
To enable DMU and allow dynamic updates of MIP keys, enter the following command:

```
dynamic-mip-key-update
```
encapsulation allow gre

Enables or disables the use of generic routing encapsulation (GRE) when establishing a MIP session. When enabled, if requested by a Mobile Node (MN), the FA requests the HA to use GRE encapsulation when establishing the MIP session. When disabled, the FA does not set the GRE bit in Agent Advertisements to the MN.

Default: GRE is enabled.

Product
PDSN, ASN GW, GGSN

Privilege
Security Administrator, Administrator

Syntax

encapsulation allow gre
no encapsulation allow gre

Usage
Use to disable or re-enable the use of GRE encapsulation for MIP sessions.

Example
To disable GRE encapsulation for MIP sessions, enter the following command;

no encapsulation allow gre

To re-enable GRE encapsulation for MIP sessions, enter the following command;

encapsulation allow gre
end

Exits the FA service configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the FA service configuration mode and returns to the context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Return to the context configuration mode.
fa-ha-spi

Configures the security parameter index (SPI) between the FA service and the HA.

Product
PDSN, ASN GW, GGSN PDIF

Privilege
Security Administrator, Administrator

Syntax

fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number
number { encrypted secret enc_secret | secret secret } [ description string | hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | monitor-ha | replay-protection { timestamp | nonce } | timestamp-tolerance tolerance ]

no fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number
number

remote-address { ha_ip_address | ip_addr_mask_combo }  

ha_ip_address: Specifies the IP address of the HA in IP v4 dotted decimal notation.
ip_addr_mask_combo: Specifies the IP address network mask bits. ip_addr_mask_combo must be specified using the form ‘IP Address/Mask Bits’ where the IP address is specified using the standard IPv4 dotted decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

spi-number number

Specifies the SPI (number) which indicates a security context between the FA and the HA in accordance with RFC 2002.

number can be configured to any integer value between 256 and 4294967295.

encrypted secret enc_secret | secret secret

Configures the shared-secret between the FA service and the HA. The secret can be either encrypted or non-encrypted.

• encrypted secret enc_secret: Specifies the encrypted shared key (enc_secret) between the FA service and the HA. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.

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

• secret secret: Specifies the shared key (secret) between the FA service and the HA. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.
**description** string

This is a description for the SPI. string must be an alpha and or numeric string of from 1 through 31 characters.

**hash-algorithm** { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5

Specifies the hash-algorithm used between the FA service and the HA.
- **hmac-md5**: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **rfc2002-md5**: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

**monitor-ha**

Default: disabled

Enables the HA monitor feature for this HA address.

To set the behavior of the HA monitor feature, refer to the **ha-monitor** command in this chapter. To disable this command (if enabled) for this HA address, re-enter the entire **fa-ha-spi** command without the **monitor-ha** keyword.

**replay-protection** { timestamp | nonce }

Default: timestamp

Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.
- **nonce**: Configures replay protection to be implemented using NONCE per RFC 2002.
- **timestamp**: Configures replay protection to be implemented using timestamps per RFC 2002.

**Important**: This keyword should only be used in conjunction with Proxy Mobile IP support.

**timestamp-tolerance** tolerance

Default: 60

Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.

**tolerance** is measured in seconds and can be configured to any integer value between 0 and 65535.

**Important**: This keyword should only be used in conjunction with Proxy Mobile IP support.

More than one of the above keywords can be entered within a single command.

**Usage**

An SPI is a security mechanism configured and shared by the FA service and the HA. Please refer to RFC 2002 for additional information.

Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a “default” SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.
**Important:** The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2048 SPIs can be configured per FA service. Use the `no` version of this command to delete a previously configured SPI.

**Example**
The following command configures the FA service to use an SPI of 512 when communicating with an HA with the IP address 192.168.0.2. The key that would be shared between the HA and the FA service is q397F65. When communicating with this HA, the FA service will also be configured to use the rfc2002-md5 hash-algorithm.

```plaintext
fa-ha-spi remote-address 192.168.0.2 spi-number 512 secret q397F65 hash-algorithm rfc2002-md5
```

The following command deletes the configured SPI of 400 for an HA with an IP address of 172.100.3.200:

```plaintext
no fa-ha-spi remote-address 172.100.3.200 spi-number 400
```
gre

Configures Generic Routing Encapsulation (GRE) parameters.

Product
PDSN, ASN GW, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gre { checksum | checksum-verify | reorder-timeout timeout | sequence-mode { none | reorder } | sequence-numbers }

no gre { checksum | checksum-verify | sequence-numbers }
```

no
Disables the specified functionality.

checksum
Default: disabled
Enables the introduction of the checksum field in outgoing GRE packets.

checksum-verify
Default: disabled
Enables verification of the GRE checksum (if present) in incoming GRE packets.

reorder-timeout timeout
Default: 100
Configures maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. `timeout` must be an integer from 0 through 5000.

sequence-mode { none | reorder }
Default: none
Configures how incoming out-of-sequence GRE packets should be handled.
none: Disables reordering of incoming out-of-sequence GRE packets.
reorder: Enables reordering of incoming out-of-sequence GRE packets.

sequence-numbers
Default: Disabled.
Enables insertion or removal of GRE sequence numbers in GRE packets.

Usage

Use this command to configure how the FA service handles GRE packets.
Example
To set maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to 500 milliseconds, enter the following command:

```
gre reorder-timeout 500
```

To enable the reordering of incoming out of sequence GRE packets, enter the following command:

```
gre sequence-mode reorder
```
ha-monitor

Configures the behavior of the HA monitor feature.

**Product**
PDSN, ASN GW, FA, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default ] ha-monitor [ interval sec | max-inactivity-time sec | num-retry num ]
[ no ] ha-monitor
```

**default**
Restores the system default setting(s) for the command/keyword(s). This command is disabled by default.

**no**
Disables the HA monitoring feature for this FA service.

**interval sec**
Default: 30
Configures the time interval before the next monitoring request message is sent to the HA.
`sec` must be a numeric value between 1 and 36000.

**max-inactivity-time sec**
Default: 60
Specifies the maximum amount of time the system will wait without receiving MIP control traffic from a HA before the HA monitoring mechanism is triggered.
`sec` must be a numeric value between 30 and 600.

**num-retry num**
Default: 5
Configures the number of time the system will attempt to send HA monitor requests before determining the HA is down and a trap is initiated.
`num` must be a numeric value between 0 and 10.

**Usage**
Use this command to set parameters for the HA monitor feature. This feature allows the AGW/FA to monitor HAs with which it has MIP sessions. The monitoring feature is triggered when the AGW/FA does not receive any MIP traffic from a HA for a configured amount of time (**max-inactivity-time**). The AGW/FA starts sending special MIP RRQ monitor messages and waits for RRP monitor message responses from the HA. The RRQ monitor messages are addressed to the HA service address. The source address of the monitor-request messages is the FA service's IP address.
The actions taken during monitoring are comprised of the following:
If no monitor response is received during the interval time (interval), the AGW retransmits the monitor message a configured number of times (num-retry).

If no response is received after retransmitting for the number configured in num-retry, the HA is considered down. The AGW/FA sends a trap (HAUnreachable) to the management station. Monitoring of this HA is stopped until a MIP control message is received from the particular HA and when the AGW/FA sends a trap (HAreachable) to the management station and starts monitoring the HA again.

When an HA receives the RRQ from an FA, it verifies the message and identifies it as a monitor message based on a special reserved NAI (in the message) and a Monitor HA CVSE in the RRQ. The HA responds with an RRP with Reply code 0x00 (accepted) and includes the Monitor HA CVSE. When the FA receives the RRP from the HA, it updates the activity for the peer HA to maintain the “up” state.

**Important:** This command only sets the behavior of the HA monitor feature. To enable the HA monitor feature for each HA address, refer to the fa-ha-spi command in this chapter. Up to 256 HAs can be monitored per system.

**Example**

The following commands set the HA monitor message interval to 45 seconds, the HA inactivity time to 60 seconds, and the number of HA monitor retries to 6:

```shell
ha-monitor interval 45
ha-monitor max-inactivity-time 60
ha-monitor num-retry 6
```
idle-timeout-mode

Controls whether Mobile IP data and control packets or only Mobile IP data resets the session idle timer.

**Product**
PDSN, ASN GW, GGSN PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

idle-timeout-mode {aggressive | normal}

- **aggressive**
  Only Mobile IP data resets the session idle timer.

- **normal**
  Both Mobile IP data and control packets reset the session idle timer.

**Usage**

Use this command to control how the session idle timer is reset.

**Example**
The following command specifies that only Mobile IP data can reset the session idle timer:

```
idle-timeout-mode aggressive
```
ignore-mip-key-data

When this is enabled, if DMU is not enabled and the MN sends a MIP-Key-Data CVSE, the FA ignores the MIP-Key-Data extension and the call is continued like a regular MIP call.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ignore-mip-key-data
no ignore-mip-key-data
```

```
no
```

Disable ignoring of MIP key data.

**Usage**

When DMU is not enabled, use this command to ignore MIP key data sent by the MN and allow the call to continue normally.

**Example**
To enable the FA to ignore MIP key data sent by the MN, enter the following command:

```
ignore-mip-key-data
```
ignore-stale-challenge

Enables the system to accept RRQs with previously used challenges. This feature is disabled by default.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

ignore-stale-challenge
no ignore-stale-challenge

Usage
Use this command to allow the FA to accept stale challenges regardless of the ID field or if other RRQs are pending.

Example
To enable this functionality in the FA service, enter the following command;

    ignore-stale-challenge

To disable this functionality, enter the following command;

    no ignore-stale-challenge
ip local-port

Configures the local User Datagram Protocol (UDP) port for the Pi interfaces’ IP socket on which to listen for Mobile IP Registration messages.

**Product**

PDSN, ASN GW, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ip local-port port#
```

*port#*

Specifies the UDP port number.

*port#* can be any integer value between 1 and 65535.

**Usage**

Specify the UDP port that should be used for communications between the FA service and the HA.

The system is shipped from the factory with the local port set to 434.

**Example**

The following command specifies a UDP port of 3950 for the FA service to use to communicate with the HA on the Pi interface:

```
ip local-port 3950
```
**isakmp**

Configures support for IPSec within the FA-service.

**Product**

PDSN, ASN GW, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
isakmp {peer-ha ha_address {crypto map map_name [ [ encrypted ] secret secret ]} |
          default { crypto map map_name [ [ encrypted ] secret secret ]}}
```

```plaintext
no isakmp { peer-ha peer_ip_address | default }
```

**no**

Deletes the reference to the crypto map for the specified HA or deletes the reference for the default crypto map.

```plaintext
peer-ha ha_address { crypto map map_name [ [ encrypted ] secret preshared_secret ] }
```

Configures a crypto map for a peer HA.

- **ha_address**: The IP address of the HA with which the FA service will establish an IPSec SA. The address must be expressed in dotted decimal format.

- **crypto map map_name**: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. `map_name` is the name of the crypto map and can be from 1 to 127 alpha and/or numeric characters.

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

- **secret secret**: The pre-shared secret that will be used during the IKE negotiation. `preshared_secret` is the secret and can be from 1 to 127 alpha and/or numeric characters.

```plaintext
default { crypto map map_name [ [ encrypted ] secret secret ] }
```

Specifies the default crypto map to use when there is no matching crypto map configured for an HA address.

- **crypto map map_name**: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. `map_name` is the name of the crypto map and can be from 1 to 127 alpha and/or numeric characters.

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

- **secret secret**: The pre-shared secret that will be used during the IKE negotiation. `preshared_secret` is the secret and can be from 1 to 127 alpha and/or numeric characters.
Usage

Use this command to configure the FA-service’s per-HA IPSec parameters. These dictate how the FA service is to establish an IPSec SA with the specified HA.

**Important:** For maximum security, it is recommended that the above command be executed for every possible HA that the FA service communicates with.

A default crypto map can also be configured using the default keyword. The default crypto map is used in the event that the AAA server returns an HA address that is not configured as an isakmp peer-ha.

**Important:** For maximum security, the default crypto map should be configured in addition to peer-ha crypto maps instead of being used to provide IPSec SAs to all HAs.

Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

Example

The following command creates a reference for an HA with the IP address 1.2.3.4 to a crypto map named map1:

```
isakmp peer-ha 1.2.3.4 crypto map map1
```

The following command deletes the crypto map reference for the HA with the IP address 1.2.3.4.

```
no isakmp peer-ha 1.2.3.4
```
limit-reg-lifetime

Enable the current default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts. When disabled, this command allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

Product
PDSN, ASN GW, GGSN PDIF

Privilege
Security Administrator, Administrator

Syntax

[no | default] limit-reg-lifetime

- **no**
  Allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

- **default**
  Enable the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Usage
Use the no keyword with this command to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.
Use the base command or the keyword to reset the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Example
Configure the FA service to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts by entering the following command:

```
no limit-reg-lifetime
```

Configure the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts by entering either of the following commands:

```
default limit-reg-lifetime
```
max-challenge-len

For mobile subscribers, the FA generates a random number and sends it to the mobile node as part of the mobile authentication extension (Mobile-Foreign Authentication extension) as described in RFC 3012. This command sets the maximum length of the FA challenge in bytes.

**Product**
PDSN, ASN GW, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
max-challenge-len length
```

*length*

Default: 16
The maximum length, in bytes, of the FA challenge. This value must be an integer in from 4 to 32.

**Usage**
Change the maximum allowed length of the randomly generated FA challenge its default of 16.

**Example**
Use the following command to change the maximum length of the FA challenge to 18 bytes:

```
max-challenge-len 18
```
mn-aaa-removal-indication

Enables the FA to remove the MN-FAC and MN-AAA extensions from RRQs. This is disabled by default.

**Product**
PDSN, ASN GW, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```markdown
mn-aaa-removal-indication
no mn-aaa-removal-indication
```

**Usage**
Enable this feature if there is no need to authenticate the subscriber at HA using MN-AAA extension.

**Example**
The following command enables the FA service to remove MN-FAC and MN-AAA extensions from RRQs:

```
mn-aaa-removal-indication
```
multiple-reg

Specifies the number of simultaneous Mobile IP sessions that will be supported for over a single PPP session.

**Product**
PDSN, ASN GW, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
multiple-reg number
```

- `number`: number can be configured to any integer value between 1 and 3.

**Usage**

Use to support multiple registrations per subscriber.
The system is shipped from the factory with the multiple simultaneous MIP sessions set to 1.

**Important:** The system will only support multiple Mobile IP sessions per subscriber if the subscriber’s mobile node has a static IP address. The system will only allow a single Mobile IP session for mobile nodes that receive a dynamically assigned IP address. In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

**Example**
The following command configures the number of supported simultaneous registrations for subscribers using this FA service to 3.

```
multiple-reg 3
```
optimize tunnel-reassembly

Configures FA to HA optimization for tunnel reassembly.

**Product**

PDSN, ASN GW, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
optimize tunnel-reassembly
no optimize tunnel-reassembly
```

**Usage**

Enabling this functionality fragments large packets prior to encapsulation for easier processing. Tunnel reassembly optimization is disabled by default.

**Important:** Cisco Systems strongly recommends that you do not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

**Important:** This functionality works best when the FA service is communicating with an HA service running in a system. However, an FA service running in the system communicating with an HA from a different manufacturer will operate correctly even if this parameter is enabled.

Use the no version of this command to disable tunnel optimization if it was previously enabled.

**Example**

The following command enables tunnel reassembly optimization:

```plaintext
optimize tunnel-reassembly
```
private-address allow-no-reverse-tunnel

This command enables the FA to allow calls with private addresses and no reverse tunneling.

Product
PDSN, ASN GW, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
private-address allow-no-reverse-tunnel
no private-address allow-no-reverse-tunnel
```

Usage

Use this command to let the FA allow sessions with private addresses that do not have the reverse tunnel bit set.

Example

To enable sessions with private addresses and no reverse tunneling, enter the following command:

```
private-address allow-no-reverse-tunnel
```
proxy-mip

Configures parameters pertaining to Proxy Mobile IP support.

Product
PDSN, ASN GW, GGSN PDIF

Privilege
Security Administrator, Administrator

Syntax

```
proxy-mip { allow | ha-failover [ max-attempts max_attempts | num-attempts-before-switching num_attempts | timeout seconds ] | max-retransmissions number | renew-percent-time renew-time | retransmission-timeout time }

no proxy-mip { allow | ha-failover }

default proxy-mip { allow | ha-failover | max-retransmissions | renew-percent-time | retransmission-timeout }
```

no
Disables FA service support for Proxy Mobile IP or HA failover for Proxy Mobile IP.

default
Restores the specified option to the default setting as described below.

allow
Default: Disabled
Enables FA service support for Proxy Mobile IP.

ha-failover [max-attempts max_attempts | num-attempts-before-switching num_attempts | timeout seconds ]
Default: Disabled
Enables HA failover for the Proxy Mobile IP feature.

- `max-attempts max_attempts` - Configures the maximum number of retransmissions of Proxy MIP control messages. `max_attempts` must be an integer from 1 through 10. Default is 4

- `num-attempts-before-switching num_attempts` - Configures the total number of RRQ attempts (including retransmissions) before failing over to the alternate HA. `num_attempts` must be an integer from 1 through 5. Default is 2.

- `timeout seconds` - Configures the retransmission timeout, in seconds, of Proxy MIP control messages when failover happens. `seconds` must be an integer from 1 through 50. Default is 2

max-retransmissions number
Default: 5
Configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
number is the maximum number of retries and can be configured to any integer value from 1 to 4294967295.

**renew-percent-time renew-time**

Default: 75

Configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

renew-time is entered as a percentage of the advertisement registration lifetime configured for the FA service. (Refer to the advertise command in this chapter). The time can be configured to any integer value from 1 to 100.

The following equation can be used to calculate renew-time:

\[
\text{renew-time} = \left( \frac{\text{duration}}{\text{lifetime}} \right) \times 100
\]

duration = The desired amount of time that can pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request

lifetime = The advertisement registration lifetime configured for the FA service.

duration £ lifetime

Default: 3

Configure the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.

time is measured in seconds and can be configured to any integer value from 1 to 100.

**Usage**

The proxy-mip command and its keywords configure the FA services support for Proxy Mobile Mobile IP. When enabled though the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

In addition to the parameters configured via this command, the HA-FA SPI(s) must also be modified to support Proxy Mobile IP. Refer to the fa-ha-spi command for more information.

**Example**

The following command configures the FA service to wait up to 5 seconds for an HA to respond prior to re-sending an a Mobile IP Registration Request message:

```
proxy-mip retransmission-timeout 5
```

If the advertisement registration lifetime configured for the FA service is 900 seconds and you want the system to send a Proxy Mobile IP Registration Renewal Request message after 500 seconds, then the following command must be executed:

```
proxy-mip renew-percent-time 50
```

Note that \( 50 = \frac{450}{900} \times 100 \).
reg-timeout

Configures the FA registration reply timeout.

**Product**

PDSN, ASN GW, GGSN PDIF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
reg-timeout time
```

*time*

Default: 45
time is measured in seconds and can be configured to any integer between 1 and 65535.

**Usage**

Configure the amount of time that the FA service will wait for a Registration Reply from an HA before the call is rejected with a reply code of 78H (registration Timeout).

**Example**

The following command configures a registration timeout of 10.

```
reg-timeout 10
```
reverse-tunnel

Enables the use of reverse tunneling for a Mobile IP sessions when requested by the mobile node.

**Product**
PDSN, ASN GW, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

reverse-tunnel

no reverse-tunnel

---

**Usage**
Reverse tunneling involves tunneling datagrams originated by the mobile node to the HA via the FA service. When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

The advantages of using reverse-tunneling:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Use the **no** option of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, then triangular routing is used.

The system is shipped from the factory with the reverse tunnel enabled.

---

**Important:** If reverse tunneling is disabled on the system and a mobile node requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

---

**Example**
The following command disables reverse-tunneling support for the FA service:

```
no reverse-tunnel
```
revocation

Enables the MIP revocation feature and configures revocation parameters.

Product
PDSN, ASN GW, GGSN PDIF

Privilege
Security Administrator, Administrator

Syntax

```
revocation { enable | max-retransmission number | negotiate-i-bit |
retransmission-timeout secs | trigger internal-failure }
```

```
no revocation enable | trigger internal-failure | negotiate-i-bit
```

```
no revocation { enable | negotiate-i-bit | trigger internal-failure }
```

Completely disables registration revocation on the FA.
Disables sending revocation messages to the HA when a session is affected by an internal task failure.

enable

Enables the MIP registration revocation feature on the FA. When enabled, if revocation is negotiated with an HA, and a MIP binding is terminated, the FA can send a Revocation message to the HA. This feature is disabled by default.

max-retransmission number

Default: 3
The maximum number of retransmissions of a Revocation message before the revocation fails. `number` must be an integer from 0 through 10.

negotiate-i-bit

Default: disabled
Enables the FA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

retransmission-timeout secs

Default: 3
The number of seconds to wait for a Revocation Acknowledgement from the HA before retransmitting the Revocation message. `secs` must be an integer from 1 through 10.

trigger internal-failure

Default: disabled
Enable sending a revocation message to the HA for all sessions that are affected by an internal task failure.

Usage
Use this command to enable or disable the MIP revocation feature on the FA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

**Example**

The following command enables Registration Revocation on the FA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 6:

```
revocation max-retransmission 6
```

The following command sets the timeout between retransmissions to 10:

```
revocation retransmission-timeout 10
```
threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per FA service.

Product
PDSN, ASN GW, GGSN

Privilege
Security Administrator, Administrator

Syntax

threshold reg-reply-error high_thresh [ clear low_thresh ]

no threshold reg-reply-error

no
Delete the alert or alarm.

high_thresh
Default: 0
The high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: You must enter a value between 1 and 100000 to trigger an alert/alarm.

clear low_thresh
Default: 0
The low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Important: You must enter a value between 1 and 100000 to trigger an alert/alarm.

Usage
Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second. Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition**: Actual number of registration reply errors > High Threshold
- **Clear condition**: Actual number of registration reply errors ≤ Low Threshold

Example
The following command configures a registration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```bash
threshold reg-reply-error 1000 clear 500
```
Chapter 99
Firewall-and-NAT Policy Configuration Mode Commands

The Firewall-and-NAT Policy Configuration Mode enables configuring Firewall-and-NAT policies.

**Important:** This configuration mode is only available in StarOS 8.1 and in StarOS 9.0 and later. This configuration mode must be used to configure Policy-based Stateful Firewall and NAT features.

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

This command creates and configures an access rule.

Product
FW, NAT

Privilege
Security Administrator, Administrator

Syntax

access-rule { no-ruledef-matches { downlink | uplink } action { deny [ charging-action charging_action ] | permit [ bypass-nat | nat-realm nat_realm ] } | priority priority { [ dynamic-only | static-and-dynamic ] access-ruledef ruledef_name { deny [ charging-action charging_action ] | permit [ [ bypass-nat | nat-realm nat_realm ] trigger open-port { port_number | range start_port to end_port } direction { both | reverse | same } ] } } }]

default access-rule no-ruledef-matches { downlink | uplink } action

no access-rule priority priority

default
Configures the default setting.
Default: uplink direction: permit; downlink direction: deny

no
Removes the access rule specified by the priority.

no-ruledef-matches
Configures action on packets with no ruledef match.

downlink
Specifies to act on downlink packets with no ruledef match.

uplink
Specifies to act on uplink packets with no ruledef match.

action
Specifies action to take on downlink/uplink packets with no ruledef match.

deny
Specifies to deny packets.

permit
Specifies to permit packets and allow the creation of data flows.
**charging-action charging_action**

Specifies the charging action. Optionally, for deny action a charging action can be configured. If a packet matches the deny rule, action is taken as configured in the charging action. If a charging action is specified, the content-ID and billing-action configured in the charging action are used. Also, the flow may be terminated (instead of just discarding the packet), if so configured in the specified charging action. `charging_action` must be an alpha and/or numeric string of 1 through 63 characters in length.

**bypass-nat**

Specifies to bypass NAT.

**nat-realm nat_realm**

Specifies the NAT realm to be used to perform NAT on subscriber packets matching the access ruledef. If the NAT realm is not specified, NAT will be bypassed. That is, NAT will not be performed on subscriber packets that are matching a ruledef with no NAT realm name configured in it. `nat_realm` must be an alpha and/or numeric string of 1 through 31 characters in length.

**priority priority**

Specifies priority of an access ruledef in the Firewall-and-NAT policy. `priority` must be an integer from 1 through 65535, and must be unique for each access ruledef in the Firewall-and-NAT policy.

```markdown
[ dynamic-only | static-and-dynamic ] access-ruledef ruledef_name
```

Specifies the access ruledef name. Optionally, the ruledef type can also be specified.

- **dynamic-only**: Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.
- **static-and-dynamic**: Static and Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is enabled by default.
- **access-ruledef ruledef_name**: Specifies the access ruledef name. `ruledef_name` must be an alpha and/or numeric string of 1 through 63 characters in length.

**trigger open-port { port_number | range start_port to end_port }**

**direction { both | reverse | same }**

Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.

- **port_number**: Specifies the auxiliary port number to open for traffic, and must be an integer from 1 through 65535.
- **range start_port to end_port**: Specifies the range of port numbers to open for subscriber traffic.
  - **start_port** must be an integer from 1 through 65535.
  - **end_port** must be an integer from 1 through 65535, and must be greater than `start_port`.
- **direction { both | reverse | same }**: Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.
Firewall-and-NAT Policy Configuration Mode Commands

access-rule

- **both**: Provides the trigger to open port for traffic in either direction of the control connection.
- **reverse**: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).
- **same**: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).

Usage

Use this command to add access ruledefs to the Firewall-and-NAT policy and configure the priority and actions for rule matching.

The policy specifies the rules to be applied on calls. The ruledefs in the policy have priorities, based on which priority matching is done.

For Stateful Firewall, the port trigger configuration is optional, and can be configured only if a rule action is permit. When a rule is matched and the rule action is permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association that matches the rule. Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic. When a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, EDR is generated.
- If the content ID is configured, UDR information is updated.
- If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets. Allowing/dropping of packets is determined in the following sequence:

- Check is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
- Access ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the `access-rule priority` configuration.
- If no access ruledef matches, the packet is allowed or dropped as per the `access-rule no-ruledef-matches` configuration.

For a packet dropped due to access ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the `access-rule priority` or the `access-rule no-ruledef-matches` command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the `flow any-error charging-action` command in the Rulebase Configuration Mode.

The GGSN can dynamically activate/deactivate dynamic ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the policy is a dynamic rule, and if the rule is enabled for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

Example

For Stateful Firewall, the following command assigns a priority of 10 to the access ruledef `test_rule`, adds it to the policy, and permits port trigger to be used for the rule to open ports in the range of 1000 to 2000 in either direction of the control connection:
access-rule priority 1 access-ruledef test_rule permit trigger open-port range 1000 to 2000 direction both
end

This command returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
exit

This command exits the current configuration mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**firewall dos-protection**

This command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.

![Important] In StarOS 8.0, this configuration is available in the ACS Configuration Mode. In StarOS 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the Rulebase Configuration Mode. In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce | ip-unaligned-timestamp | mime-flood | port-scan | source-router | tcp-window-containment | teardrop | winnuke }
```

**default firewall dos-protection**

- **no**
  Disables Stateful Firewall protection for subscribers against the specified DoS attack(s).

- **default**
  Disables Stateful Firewall protection for subscribers against all DoS attacks.

- **all**
  Enables Stateful Firewall protection for subscribers against all DoS attacks supported by the Stateful Firewall service.

- **flooding { icmp | tcp-syn | udp }**
  Enables protection against the specified flooding attack:

  - **icmp**
    Enables protection against ICMP Flood attack

  - **tcp-syn**
    Enables protection against TCP Syn Flood attack

  - **udp**
    Enables protection against UDP Flood attack

- **ftp-bounce**
  Enables protection against FTP Bounce attacks.

- **ip-unaligned-timestamp**
  Enables protection against IP Unaligned Timestamp attacks.
Enables protection against HTTP Multiple Internet Mail Extension (MIME) header flooding attacks.

Enables protection against Port Scan attacks.

Enables protection against TCP sequence number out-of-range attacks.

Enables protection against IP Source Route IP Option attacks.

Enables protection against Teardrop attacks.

Enables protection against WIN-NUKE attacks.

Use this command to enable Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

Important: DoS attacks are detected only in the downlink direction.

The following command enables protection from all supported DoS attacks:

```
firwall dos-protection all
```
firewall flooding

This command configures Stateful Firewall protection from Packet Flooding attacks.

**Important:** In StarOS 8.0, this configuration is available in the ACS Configuration Mode. In StarOS 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the Rulebase Configuration Mode. In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

**Product:**
FW

**Privilege:**
Security Administrator, Administrator

**Syntax:**

```
firewall flooding { protocol { icmp | tcp-syn | udp } packet limit packets } | sampling-interval interval }

default firewall flooding { protocol { icmp | tcp-syn | udp } packet limit } | sampling-interval }

default
Configures the default setting for the specified configuration.

protocol { icmp | tcp-syn | udp }
Specifies the transport protocol:
- icmp: Configuration for ICMP protocol.
- tcp-syn: Configuration for TCP-SYN packet limit.
- udp: Configuration for UDP protocol.

packet limit packets
Specifies the maximum number of specified packets a subscriber can receive during a sampling interval. packets must be an integer from 1 through 4294967295. Default: 1000 packets per sampling interval for all protocols.

sampling-interval interval
Specifies the flooding sampling interval, in seconds. interval must be an integer from 1 through 60. Default: 1 second
The maximum sampling-interval configurable is 60 seconds.

**Usage**

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.
Example
The following command ensures a subscriber will not receive more than 1000 ICMP packets per sampling interval:

```
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IPs, those packets will be limited to 1000 packets per sampling interval. This way only “suspected” malicious packets are limited and not “legitimate” packets.

```
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 TCP-Syn packets per sampling interval.

```
firewall flooding protocol tcp-syn packet limit 1000
```

The following command specifies a flooding sampling interval of 1 second:

```
firewall flooding sampling-interval 1
```
**firewall icmp-checksum-error**

This command configures Stateful Firewall action on packets with ICMP Checksum errors.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall icmp-checksum-error { drop | permit }
```

**default firewall icmp-checksum-error**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures the default setting. Default: drop</td>
</tr>
<tr>
<td>drop</td>
<td>Specifies to drop packets with ICMP Checksum errors.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies to permit packets with ICMP Checksum errors.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure Stateful Firewall action on packets with ICMP Checksum errors. This CLI also applies to ICMP packets with Inner IP Checksum error.

For NAT-only calls, packets with ICMP errors are dropped, and other packets are allowed.

**Example**

The following command configures Stateful Firewall to drop packets with ICMP Checksum errors:

```
firewall icmp-checksum-error drop
```
**firewall icmp-destination-unreachable-message-threshold**

This command configures a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.

---

**Important:** In StarOS 8.0, this configuration is available in the ACS Configuration Mode. In StarOS 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the Rulebase Configuration Mode. In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall icmp-destination-unreachable-message-threshold messages then-block-server

{ default | no } firewall icmp-destination-unreachable-message-threshold
```

- **default**
  - Configures the default setting.
  - Default: No limit

- **no**
  - Removes the previous configuration.

- **messages**
  - Specifies the threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. `messages` must be an integer from 1 through 100.

**Usage**

Use this command to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked. Some servers that run QChat ignore the ICMP error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.

**Example**

The following command configures a threshold of 10 ICMP error messages:

```plaintext
firewall icmp-destination-unreachable-message-threshold 10 then-block-server
```
**firewall icmp-fsm**

This command enables/disables Stateful Firewall’s ICMP Finite State Machine (FSM).

**Product**

FW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ default | no ] firewall icmp-fsm
```

- **default**
  - Configures the default setting.
  - Default: Enabled. Same as `firewall icmp-fsm`

- **no**
  - Disables Stateful Firewall ICMP FSM checks.

**Usage**

Use this command to enable/disable Stateful Firewall ICMP FSM checks. When Stateful Firewall and ICMP FSM are enabled, ICMP reply messages for which there is no saved ICMP request message are discarded. ICMP error messages (i.e., messages containing an embedded message) for which there is no saved flow for the embedded message are discarded.

**Example**

The following command disables Stateful Firewall’s ICMP FSM checks:

```
no firewall icmp-fsm
```
**firewall ip-reassembly-failure**

This command configures Stateful Firewall action on packets involved in IP Reassembly Failure scenarios.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
fir iewall ip-reassembly-failure { drop | permit }
default fireplace l ip-reassembly-failure
```

- **default**
  - Configures the default setting.
  - Default: `permit`

- **drop**
  - Specifies to drop packets involved in IP reassembly failure scenarios.

- **permit**
  - Specifies to permit packets involved in IP reassembly failure scenarios.

**Usage**
Use this command to configure Stateful Firewall action on packets involved in IP reassembly failure scenarios such as missing fragments, overlapping offset, etc.
For NAT-only calls, packets involved in IP reassembly failure scenarios are dropped.

**Example**
The following command specifies to drop packets involved in IP reassembly failure scenarios:
```
fir iewall ip-reassembly-failure drop
```
firewall malformed-packets

This command configures Stateful Firewall action on malformed packets.

Product
FW

Privilege
Security Administrator, Administrator

Syntax

firewall malformed-packets { drop | permit }

default firewall malformed-packets

default
Configures the default setting.
Default: permit

drop
Specifies to drop malformed packets.

permit
Specifies to permit malformed packets.

Usage
Use this command to configure Stateful Firewall action on malformed packets. For NAT-only calls, malformed packets are always permitted.

Example
The following command specifies Stateful Firewall to drop malformed packets:

firewall malformed-packets drop
firewall max-ip-packet-size

This command configures the maximum IP packet size (after IP reassembly) allowed over Stateful Firewall.

**Important:** In StarOS 8.0, this configuration is available in the ACS Configuration Mode. In StarOS 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the Rulebase Configuration Mode. In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

**Syntax**

```
firewall max-ip-packet-size packet_size protocol { icmp | non-icmp }
```

```
default firewall max-ip-packet-size protocol { icmp | non-icmp }
```

**Syntax**

```
default
```

Configures the default setting.
Default: 65535 bytes (for both ICMP and non-ICMP)

```
packet_size
```

Specifies the maximum packet size allowed.
```
packet_size must be an integer from 30000 through 65535.
```

```
protocol { icmp | non-icmp }
```

Specifies the transport protocol:
```
•icmp: Configuration for ICMP protocol.
```
```
•non-icmp: Configuration for protocols other than ICMP.
```

**Usage**

Use this command to configure the maximum IP packet size allowed for ICMP and non-ICMP packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for “Jolt” and “Ping-Of-Death” attacks.

**Example**

The following command allows a maximum packet size of 60000 for ICMP protocol:

```
firewall max-ip-packet-size 60000 protocol icmp
```
**firewall mime-flood**

This command configures Stateful Firewall protection from MIME Flood attacks.

⚠️ **Important:** In StarOS 8.0, this configuration is available in the ACS Configuration Mode. In StarOS 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the Rulebase Configuration Mode. In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

**Product**

FW

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
firewall mime-flood { http-headers-limit max_limit | max-http-header-field-size max_size }
default firewall mime-flood { http-headers-limit | max-http-header-field-size }
```

**default**

Configures the default setting for the specified parameter.

**http-headers-limit max_limit**

Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.

- `max_limit` must be an integer from 1 through 256.
- Default: 16

**max-http-header-field-size max_size**

Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.

- `max_size` must be an integer from 1 through 8192.
- Default: 4096 bytes

**Usage**

Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks. This command is only effective if Stateful Firewall DoS protection for MIME flood attacks has been enabled using the `firewall dos-protection mime-flood` command, and the `route` command has been configured to send HTTP packets to the HTTP analyzer.

**Example**

The following command sets the maximum number of headers allowed in an HTTP packet to 100:
The following command sets the maximum header field size allowed in the HTTP header to 1000 bytes:

```
firewall mime-flood max-http-header-field-size 1000
```
**firewall policy**

This command enables/disables Stateful Firewall support in a Firewall-and-NAT policy.

**Important:** In StarOS 8.0, this configuration is available in the ACS Configuration Mode. In StarOS 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the Rulebase Configuration Mode. In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

---

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall policy firewall-required

no firewall policy
```

**Usage**
Use this command to enable/disable Stateful Firewall support for all subscribers using a Firewall-and-NAT policy.

**Example**
The following command enables Stateful Firewall support in a Firewall-and-NAT policy:

```plaintext
firewall policy firewall-required
```

The following command disables Stateful Firewall support in a Firewall-and-NAT policy:

```plaintext
no firewall policy
```
**firewall tcp-checksum-error**

This command configures Stateful Firewall action on packets with TCP Checksum error.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall tcp-checksum-error { drop | permit }
```

```
default firewall tcp-checksum-error
```

**Usage**

Use this command to configure Stateful Firewall action on packets with TCP Checksum error. For NAT-only calls, packets with TCP Checksum errors are permitted.

**Example**

The following command specifies Stateful Firewall to drop packets with TCP Checksum errors:

```
firewall tcp-checksum-error drop
```
firewall tcp-first-packet-non-syn

This command configures Stateful Firewall action on TCP flows starting with a non-SYN packet.

Product
FW

Privilege
Security Administrator, Administrator

Syntax

```
firewall tcp-first-packet-non-syn { drop | reset }
```

default firewall tcp-first-packet-non-syn

```
default
Configures the default setting.
Default: `drop`
```

```
drop
Specifies to drop the non-SYN packet.
```

```
reset
Specifies to send reset.
```

Usage

Use this command to configure Stateful Firewall action on TCP flows starting with a non-SYN packet.

Example

For flows starting with a non-SYN packet, the following command specifies Stateful Firewall to drop the non-SYN packet:

```
firewall tcp-first-packet-non-syn drop
```
**firewall tcp-fsm**

This command enables/disables Stateful Firewall’s TCP Finite State Machine (FSM).

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall tcp-fsm [ first-packet-non-syn { drop | permit | send-reset } ] [ default | no ]
```

- **default**
  Configures the default setting.
  Default: `firewall tcp-fsm first-packet-non-syn drop`

- **no**
  Disables Stateful Firewall’s TCP FSM.

- **first-packet-non-syn { drop | permit | send-reset }**
  Specifies Stateful Firewall action on TCP flows starting with a non-SYN packet:
  - **drop**: Specifies to drop the packet.
  - **permit**: Specifies to permit the packet.
  - **send-reset**: Specifies to drop the packet and send TCP RST.
  Default: `drop`

**Usage**
Use this command to enable/disable Stateful Firewall’s TCP FSM checks. When Stateful Firewall and TCP FSM are enabled, state of the TCP session is checked to decide whether to forward TCP packets.

**Example**
The following command enables TCP FSM, and configures action to take on TCP flows starting with a non-SYN packet to drop the packet:

`firewall tcp-fsm first-packet-non-syn drop`
**firewall tcp-idle-timeout-action**

This command configures action on TCP idle timeout expiry.

**Product**
FW, NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall tcp-idle-timeout-action { drop | reset }
{ default | no } firewall tcp-idle-timeout-action
```

---

**default**
Configures the default setting.
Default: `reset`

---

**no**
Configures the TCP idle timeout expiry action to reset.

---

**drop | reset**
Specifies the action to take on TCP idle timeout expiry.
- **drop**: Drops the session.
- **reset**: Sends TCP RST. When configured to reset, the session is dropped, and the system can avoid packets arriving for the idle flow from getting dropped.

**Usage**
Use this command to configure action to take on TCP idle timeout expiry.

**Example**
The following command configures action to take on TCP idle timeout expiry to drop:

```
firewall tcp-idle-timeout-action drop
```
firewall tcp-options-error

This command configures Stateful Firewall action on packets with TCP Option errors.

Product
FW

Privileges
Security Administrator, Administrator

Syntax

```
firewall tcp-options-error { drop | permit }

default firewall tcp-options-error
```

- **default**
  
  Configures the default setting.
  
  Default: `permit`

- **drop**
  
  Specifies to drop packets with TCP Option errors.

- **permit**
  
  Specifies to permit packets with TCP Option errors.

Usage

Use this command to configure Stateful Firewall action on packets with TCP Option errors.

Example

The following command configures Stateful Firewall to drop packets with TCP Option errors:

```
firweall tcp-options-error drop
```
**firewall tcp-reset-message-threshold**

This command configures a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall tcp-reset-message-threshold messages then-block-server
	default | no firewall tcp-reset-message-threshold
```

- **default**
  Configures the default setting.
  Default: Disabled

- **no**
  Disables the configuration.

- **messages**
  Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. `messages` must be an integer from 1 through 100.

**Usage**

Use this command to configure a threshold on the number of TCP reset messages (TCP RST+ACK) sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked. This configuration enables QCHAT noise suppression for TCP.

**Example**

The following command sets the threshold on the number of TCP reset messages to 10:

```
firewall tcp-reset-message-threshold 10 then-block-server
```
firewall tcp-syn-flood-intercept

This command configures TCP SYN intercept parameters for protection against TCP SYN flooding attacks.

**Important:** In StarOS 8.0, this configuration is available in the ACS Configuration Mode. In StarOS 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the Rulebase Configuration Mode. In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall tcp-syn-flood-intercept { mode { none | watch [ aggressive ] } | watch-timeout intercept_watch_timeout }
```

default firewall tcp-syn-flood-intercept { mode | watch-timeout }

default
Confignes the default settings for SYN Flood DoS protection.

```
mode { none | watch [ aggressive ] }
```

Specifies the TCP SYN flood intercept mode:

- **none**: Disables the TCP SYN Flood Intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. The Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, the Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.

- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

Default: **none**

```
watch-timeout intercept_watch_timeout
```

Specifies the TCP intercept watch timeout, in seconds.

*intercept_watch_timeout* must be an integer from 5 through 30.

Default: 30
Usage
This TCP intercept functionality provides protection against TCP SYN Flooding attacks. This command enables and configures TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the `dos-protection` command.

The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

Example
The following command sets the intercept watch timeout setting to 15 seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 15
```
**firewall tcp-syn-with-ecn-cwr**

This command configures Stateful Firewall action on TCP SYN packets with either ECN or CWR flag set.

**Product**
FW

**Privileges**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall tcp-syn-with-ecn-cwr { drop | permit }
default firewall tcp-syn-with-ecn-cwr
```

- **default**
  Configures the default setting.
  Default: `permit`

- **drop**
  Specifies to drop TCP SYN packets with either ECN or CWR flag set.

- **permit**
  Specifies to permit TCP SYN packets with either ECN or CWR flag set.

**Usage**
Use this command to configure Stateful Firewall action on receiving a TCP SYN packet with either ECN or CWR flag set.

**Example**
The following command configures Stateful Firewall to drop TCP SYN packets with ECN / CWR flag set:

```plaintext
firewall tcp-syn-with-ecn-cwr drop
```
**firewall udp-checksum-error**

This command configures Stateful Firewall action on packets with UDP Checksum error.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
fir**** firewall udp-checksum-error { drop | permit }
default firewall udp-checksum-error
```

- **default**
  Configures the default setting.
  Default: **drop**

- **drop**
  Specifies to drop packets with UDP Checksum error.

- **permit**
  Specifies to permit packets with UDP Checksum error.

**Usage**
Use this command to configure Stateful Firewall action on packets with UDP Checksum error.
For NAT-only calls, packets with UDP Checksum error are permitted.

**Example**
The following command specifies to drop packets with UDP Checksum error:

```
fir**** firewall udp-checksum-error drop
```
**firewall validate-ip-options**

This command enables / disables the Stateful Firewall validation of IP options for errors.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] firewall validate-ip-options
```

- **default**
  Configures the default setting.
  Default: Disabled. Same as `no firewall validate-ip-options`

- **no**
  Disables validation of IP options.

**Usage**

Use this command to enable / disable Stateful Firewall validation of IP options. When enabled, Stateful Firewall will drop packets with IP option errors. For NAT calls, validation of IP Options is disabled.

**Example**
The following command enables validation of IP options:

```
firewall validate-ip-options
```
**nat binding-record**

This command configures the generation of NAT Binding Records.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nat binding-record edr-format edr_format [ port-chunk-allocation ] [ port-chunk-release ]

{ default | no } nat binding-record
```

- **default**
  Configures the default setting.
  Default: `port-chunk-release`

- **no**
  Disables generating NAT Binding Records.

- **edr-format edr_format**
  Specifies the EDR format name.
  `edr_format` must be an alpha and/or numeric string of 1 through 63 characters in length.

- **port-chunk-allocation**
  Specifies generating NAT Binding Records when a port-chunk is allocated.

- **port-chunk-release**
  Specifies generating NAT Binding Record when a port-chunk is released.

**Usage**
Use this command to configure the generation of NAT Binding Records.

**Example**
The following command configures an EDR format named `test123` and specifies generating NAT Binding Records when a port chunk is allocated:

```
nat binding-record edr-format test123 port-chunk-allocation
```
nat policy

This command enables/disables Network Address Translation (NAT) support in a Firewall-and-NAT policy.

**Important:** In StarOS 8.3, this configuration is available in the Rulebase Configuration Mode.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nat policy nat-required [ default-nat-realm nat_realm_name ]

no nat policy
```

- **no**
  - Disables NAT support in the Firewall-and-NAT policy.

- **nat-required**
  - Enables NAT support in the Firewall-and-NAT policy.

- **default-nat-realm nat_realm_name**
  - Specifies the default NAT realm for the Firewall-and-NAT policy.
    - `nat_realm_name` must be the name of an existing NAT realm, and must be an alpha and/or numeric string of 1 through 31 characters in length.

**Usage**

Use this command to enable/disable NAT support for all subscribers using a Firewall-and-NAT policy. In StarOS 8.1, to enable NAT support for a subscriber, Stateful Firewall must also be enabled for that subscriber. See the `firewall policy` CLI command.

Once NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms specified in the rules. See the `access-rule` CLI command.

You can enable/disable NAT at any time, however the changed NAT status will not be applied to active calls. The new NAT status will only be applied to new calls.

**Example**

The following command enables NAT support in a Firewall-and-NAT policy:

```
nat policy nat-required
```

The following command disables NAT support in a Firewall-and-NAT policy:

```
no nat policy
```
nat private-ip-flow-timeout

This command configures the Private IP NPU flow timeout setting.

Product
NAT

Privilege
Security Administrator, Administrator

Syntax

nat private-ip-flow-timeout timeout
{ default | no } nat private-ip-flow-timeout

**default**
Configures the default setting.
Default: 180 seconds

**no**
Disables the Private IP NPU flow timeout configuration.
When disabled, the flow is installed at call setup and will be removed only when the subscriber disconnects.

**timeout**
Specifies the Private IP NPU flow timeout period in seconds.
*timeout* must be an integer from 180 through 86400.

Usage
Use this command to configure the Private IP NPU flow timeout setting.
For NAT-enabled calls, by default, the downlink private IP NPU flow will not be installed at call setup for a subscriber session. The flow will only be installed on demand. When there is no traffic on the private flow, the private IP flow will be removed after the configurable timeout period.

Example
The following command configures the Private IP NPU flow timeout setting to 36000 seconds:

```
nat private-ip-flow-timeout 36000
```
nat suppress-aaa-update

This command suppresses sending NAT Bind Update (NBU) to the AAA server when PPP disconnect happens.

Important: This command is customer-specific. For more information please contact your local service representative.

Product
NAT

Privilege
Security Administrator, Administrator

Syntax

nat suppress-aaa-update call-termination

default nat suppress-aaa-update

default
Configure the default setting.
Default: No suppression of AAA updates.

Usage
Use this command to suppress sending of NBU to the AAA server when PPP disconnect happens, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NBU are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

Example
The following command suppresses the sending of NBU to the AAA server:

    nat suppress-aaa-update call-termination
Chapter 100
Firewall Ruledef Configuration Mode Commands

The Firewall Ruledef Configuration Mode is used to configure and manage Access/Stateful Firewall rule definitions.

![Diagram]

- Exec Mode
  - active-charging
    - service name
  - ACS Configuration Mode
    - firewall ruledef
      - name
  - ACS Firewall Ruledef Configuration Mode
bearer 3gpp apn

This command configures an access/firewall ruledef to analyze user traffic based on APN bearer.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] bearer 3gpp apn [ case-sensitive ] operator value

no
Removes previously configured bearer ruledef.

case-sensitive
This keyword makes the rule case sensitive.
By default, ruledefs are not case sensitive.
Default: Disabled

operator
Specifies how to logically match the APN name.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• =: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

value
The APN name to match in bearer flow.
value must be an alpha and/or numeric string of 1 through 62 characters in length, and can include punctuation characters.

Usage
Use this command to specify an access/firewall ruledef to analyze user traffic based on APN name.

Example
The following command creates an access/firewall ruledef for analyzing user traffic for an APN named apn12:
bearer 3gpp apn = apn12
**bearer 3gpp imsi**

This command configures an access/firewall ruledef to analyze user traffic based on International Mobile Station Identification (IMSI) number in bearer flow.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer 3gpp imsi { operator msid | { !range | range } imsi-pool imsi_pool }
```

- **no**
  Removes previously configured bearer ruledef.

- **operator**
  Specifies how to logically match the MSID.
  `operator` must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **msid**
  Specifies the Mobile Station Identifier.

- `{ !range | range } imsi-pool imsi_pool`
  `{ !range | range }`: Specifies the range criteria:
    - !=range: Not in the range of
    - range: In the range of
  `imsi-pool imsi_pool`: Specifies the IMSI pool name. `imsi_pool` must be a string of 1 through 63 characters in length.

**Usage**
Use this command to specify an access/firewall ruledef to analyze user traffic based on IMSI number of mobile station.

**Example**
The following command creates an access/firewall ruledef to analyze user traffic for the IMSI number 9198838330912:

```
bearer 3gpp imsi = 9198838330912
```
bearer username

This command configures an access/firewall ruledef to analyze user traffic based on user name of the bearer flow.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer username [ case-sensitive ] operator value
```

- **no**
  Removes previously configured bearer ruledef.

- **case-sensitive**
  This keyword makes the rule case sensitive.
  By default, ruledefs are not case sensitive.
  Default: Disabled

- **operator**
  Specifies how to logically match the MSID.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **value**
  Specifies the user name.
  `value` must be an alpha and/or numeric string of 1 through 127 characters in length.

**Usage**

Use this command to specify a access/firewall ruledef to analyze user traffic based on user name of the bearer flow.

**Example**

The following command creates an access/firewall ruledef for analyzing user traffic for the user name `user12`:
bearer username = user12
create-log-record

This command enables/disables Firewall ruledef logging.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] create-log-record

  no
  Disables Firewall ruledef logging.

Usage
Use this command to enable/disable Firewall ruledef logging.

Example
The following command enables Firewall ruledef logging:

  create-log-record

The following command disables Firewall ruledef logging:

  no create-log-record
end

This command exits the current configuration mode, and returns to the Executive mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to change to the Executive mode.
exit

This command exits the current configuration mode, and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**icmp any-match**

This command configures an access/firewall ruledef to match any ICMP traffic for the user.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] icmp any-match  operator  condition
```

- **no**
  
  Removes previously configured ICMP any-match ruledef.

- **operator**
  
  Specifies how to logically match the analyzed state.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  
  Specifies the condition to be matched for the user traffic.
  
  `condition` must be one of the following:
  
  - `FALSE`: Specified condition is FALSE.
  - `TRUE`: Specified condition is TRUE.

**Usage**

Use this command to specify an access/firewall ruledef to match any ICMP traffic of the user.

**Example**

The following command creates an access/firewall ruledef to match any non-ICMP traffic of the user:

```
icmp any-match = FALSE
```
**icmp code**

This command configures an access/firewall ruledef to analyze user traffic based on ICMP code.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] icmp code operator code
```

- **no**
  Removes previously configured ICMP code ruledef.

- **operator**
  Specifies how to logically match the ICMP code.
  *operator* must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **code**
  Specifies the ICMP code.
  *code* must be an integer from 0 through 255.

**Usage**

Use this command to define an access/firewall ruledef to analyze user traffic based on the ICMP code.

**Example**

The following command creates an access/firewall ruledef for analyzing user traffic using the ICMP code as 23:

```
icmp code = 23
```
icmp type

This command configures an access/firewall ruledef to analyze user traffic based on ICMP type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] icmp type operator type
```

- **no**
  Removes previously configured ICMP type ruledef.

- **operator**
  Specifies how to logically match the ICMP type.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `=`: Equals
  - `=>`: Greater than or equals

- **type**
  Specifies the ICMP type.
  `type` must be an integer from 0 through 255.
  For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

**Usage**

Use this command to define an access/firewall ruledef to analyze user traffic based on the ICMP type.

**Example**

The following command creates an access/firewall ruledef for analyzing user traffic using an ICMP type as 123:

```
icmp type = 123
```
ip any-match

This command configures an access/firewall ruledef to match any IP traffic for the user.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip any-match operator condition

no
Removes previously configured IP any-match ruledef.

operator
Specifies how to logically match the analyzed state. operator must be one of the following:
  • !=: Does not equal
  • ==: Equals

condition
Specifies the condition to be matched for the user traffic. condition must be one of the following:
  • FALSE: Specified condition is FALSE.
  • TRUE: Specified condition is TRUE.

Usage

Use this command to specify an access/firewall ruledef to match any IP traffic of the user.

Example

The following command creates an access/firewall ruledef to match any non-IP traffic of the user:

    ip any-match = FALSE
ip downlink

This command configures an access/firewall ruledef to analyze user traffic based on IP packet flow in downlink direction (to subscriber).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip downlink operator condition

no
Removes previously configured IP ruledef.

operator
Specifies how to logically match the packet flow direction.
operator must be one of the following:
  • !=: Does not equal
  • ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
  • TRUE: Analyzed
  • FALSE: Not analyzed

Usage
Use this command to define an access/firewall ruledef to analyze user traffic based on the IP packet flow direction as downlink.

Example
The following command creates firewall ruledef for analyzing user traffic using an IP packet direction to downlink (to subscriber):

    ip downlink = TRUE
**ip dst-address**

This command configures an access/firewall ruledef to analyze user traffic based on IP destination address.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ip dst-address { operator { ip_address | ip_address/mask } | { !range | range } host-pool host_pool }
```

- **no**
  Removes previously configured IP destination address ruledef.

- **operator { ip_address | ip_address/mask }**
  **operator** specifies how to logically match the IP destination address. **operator** must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `>=`: greater than or equals

  **ip_address**: Specifies the IP address of destination node for outgoing traffic in IPv4 or IPv6 standard notation. **ip_address** must be the IP address in dotted decimal notation for IPv4, or in colon notation for IPv6.

  **ip_address/mask**: Specifies the IP address of destination node for outgoing traffic in IPv4 or IPv6 standard notation with subnet mask bit. **ip_address/mask** must be the IP address in dotted decimal notation for IPv4, or in colon notation for IPv6 with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

- **{ !range | range } host-pool host_pool**
  **{ !range | range }**: Specifies the range criteria:
    - `!range`: Not in the range of
    - `range`: In the range of

  **host-pool host_pool**: Specifies the host pool name. **host_pool** must be a string of 1 through 63 characters in length.

**Usage**

Use this command to specify an access/firewall ruledef to analyze user traffic based on the IP destination address.

**Example**
The following command creates IP ruledef for analyzing user traffic using an IP destination address of 1.1.1.1:

```
ip dst-address = 1.1.1.1
```
ip protocol

This command configures an access/firewall ruledef to analyze user traffic based on the protocol being transported by IP packets.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
[ no ] ip protocol { { operator { protocol | protocol_assignment } } } | { operatorprotocol_assignment } }
```

- **no**
  Removes previously configured IP protocol address ruledef.

- **operator { protocol | protocol_assignment }**
  - **operator**: Specifies how to logically match the IP protocol. **operator** must be one of the following:
    - `! =`: Does not equal
    - `= =`: Equals
  - **protocol**: Specifies the protocol by name. **protocol** must be one of the following:
    - `ah`
    - `esp`
    - `gre`
    - `icmp`
    - `tcp`
    - `udp`
  - **protocol_assignment**: Specifies the protocol by assignment number. **protocol_assignment** must be an integer from 0 through 255 (e.g., 1 for ICMP, 6 for TCP, and 17 for UDP).

- **operator protocol_assignment**
  - **operator**: Specifies how to logically match the IP protocol. **operator** must be one of the following:
    - `<`: less than
    - `<=`: less than or equals
    - `> =`: greater than or equals
  - **protocol_assignment**: Specifies the protocol by assignment number. **protocol_assignment** must be an integer from 0 through 255 (e.g., 1 for ICMP, 6 for TCP, and 17 for UDP).

Usage

Use this command to specify an access/firewall ruledef to analyze user traffic based on the IP protocol.
Example
The following command creates IP ruledef for analyzing user traffic using a protocol assignment of 1:

```
ip protocol = 1
```
ip src-address

This command configures an access/firewall ruledef to analyze user traffic based on IP source address.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip src-address { operator { ip_address | ip_address/mask } | { !range | range } host-pool host_pool }

no
Removes previously configured IP destination address ruledef.

operator { ip_address | ip_address/mask }
operator: Specifies how to logically match the IP source address. operator must be one of the following:
• !: does not equal
• <=: less than or equals
• =: equals
• =>: greater than or equals

ip_address: Specifies the IP address of source node for incoming traffic in IPv4 or IPv6 standard notation. ip_address must be the IP address in dotted decimal notation for IPv4, or in colon notation for IPv6.

ip_address/mask: Specifies the IP address of source node for incoming traffic in IPv4 or IPv6 standard notation with subnet mask bit. ip_address/mask must be the IP address in dotted decimal notation for IPv4, or in colon notation for IPv6 with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool host_pool

!range | range: Specifies the range criteria:
• !range: Not in the range of
• range: In the range of

host-pool host_pool: Specifies the host pool name. host_pool must be a string of 1 through 63 characters in length.

Usage
Use this command to specify an access/firewall ruledef to analyze user traffic based on the IP source address.

Example
The following command creates IP ruledef for analyzing user traffic using an IP source address of 1.1.1.1:

OL-22948-01
Cisco ASR 5000 Series Command Line Interface Reference
ip src-address = 1.1.1.1
ip uplink

This command configures an access/firewall ruledef to analyze user traffic based on IP packet flow in uplink direction (from subscriber).

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] ip uplink operator condition
```

- **no**
  Removes previously configured IP uplink match ruledef.

- **operator**
  Specifies how to logically match the IP packet flow direction. `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match. `condition` must be one of the following:
  - `true`: Not analyzed
  - `false`: Analyzed

Usage
Use this command to define an access/firewall ruledef to analyze user traffic based on the IP packet flow direction as uplink.

Example
The following command creates firewall ruledef for analyzing user traffic using an IP packet direction to uplink (from subscriber):

```
ip uplink = TRUE
```
tcp any-match

This command configures an access/firewall ruledef to match any TCP traffic for the user.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp any-match operator condition

no
Removes previously configured TCP any-match ruledef.

operator
Specifies how to logically match the analyzed state. operator must be one of the following:
- • ! =: does not equal
- • =: equals

condition
Specifies the condition to be matched for the user traffic. condition must be one of the following:
- • FALSE: Specified condition is FALSE.
- • TRUE: Specified condition is TRUE.

Usage
Use this command to specify an access/firewall ruledef to match any TCP traffic of the user.

Example
The following command creates an access/firewall ruledef to match any non-TCP traffic of the user:

tcp any-match = FALSE
tcp dst-port

This command configures an access/firewall ruledef to analyze user traffic based on destination TCP port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }

no
Removes the previously configured destination TCP port ruledef.

operator
Specifies how to logically match the port number.
operator must be one of the following:

• !=: Does not equal
• <=: Less than or equals
• =: Equals
• >=: Greater than or equals

port_number
Specifies the port number to match.
port_number must be an integer from 1 to 65535.

range | !range
Specifies the range criteria:

• !range: Not in the range
• range: In the range

start_range to end_range
Specifies the starting and ending port numbers for the range of destination TCP ports.
start_range must be an integer from 1 through 65535.
enrange must be an integer from 1 through 65535, and must be greater than start_range

port-map port_map
Specifies name of the port-map for the port range.
port_map must be a string of 1 through 63 characters in length.

Usage
Use this command to specify an access/firewall ruledef to analyze user traffic based on destination TCP port.

**Example**
The following command creates an access/firewall ruledef for analyzing user traffic matching destination port for TCP as 10:

```
tcp dst-port = 10
```
### tcp either-port

This command configures an access/firewall ruledef to analyze user traffic based on either (destination or source) TCP ports.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] tcp either-port { operator port_number | ( !range | range ) { start_range
to end_range | port-map port_map } }
```

---

**no**

Removes previously configured TCP either-port (destination or source) ruledef.

---

**operator**

Specifies how to logically match the port number.

- `!=`: Does not equal
- `<=`: Less than or equals
- `=`: Equals
- `>=`: Greater than or equals

---

**port_number**

Specifies the port number to match.

- `port_number` must be an integer from 1 through 65535.

---

**range | !range**

Specifies the range criteria:

- `!range`: Not in the range
- `range`: In the range

---

**start_range to end_range**

Specifies the starting and ending port numbers for the port range.

- `start_range` must be an integer from 1 through 65535.
- `end_range` must be an integer from 1 through 65535, and must be greater than `start_range`.

---

**port-map port_map**

Specifies name of the port-map for the port range.

- `port_map` must be a string of 1 through 63 characters in length.
Usage
Use this command to specify an access/firewall ruledef to analyze user traffic based on either TCP port.

Example
The following command creates an access/firewall ruledef for analyzing user traffic matching destination or source port for TCP as 10:

```
tcp either-port = 10
```
tcp src-port

This command configures an access/firewall ruledef to analyze user traffic based on source TCP port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] tcp src-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes previously configured source TCP port ruledef.

- **operator**
  Specifies how to logically match the port number.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 to 65535.

- **range | !range**
  Specifies the range criteria:
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  `start_range` must be an integer from 1 through 65535.
  `end_range` must be an integer from 1 through 65535, and must be greater than `start_range`.

- **port-map port_map**
  Specifies name of the port-map for the port range.
  `port_map` must be a string of 1 through 63 characters in length.

**Usage**
Use this command to specify an access/firewall ruledef to analyze user traffic based on source TCP port.

Example
The following command creates an access/firewall ruledef for analyzing user traffic matching source port for TCP as 10:

```
tcp src-port = 10
```
udp any-match

This command configures an access/firewall ruledef to match any UDP traffic for the user.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] udp any-match operator condition

no
Removes previously configured UDP any-match ruledef.

operator
Specifies how to logically match the analyzed state.
operator must be one of the following:
  * =: does not equal
  * =: equals

condition
Specifies the condition to be matched for the user traffic.
condition must be one of the following:
  * FALSE: Specified condition is FALSE.
  * TRUE: Specified condition is TRUE.

Usage
Use this command to specify an access/firewall ruledef to match any UDP traffic of the user.

Example
The following command creates an access/firewall ruledef to match any UDP traffic of the user:

    udp any-match = TRUE
udp dst-port

This command configures an access/firewall ruledef to analyze user traffic based on destination UDP port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] udp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes previously configured destination UDP ports ruledef.

- **operator**
  Specifies how to logically match the port number.
  *operator* must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  *port_number* must be an integer from 1 through 65535.

- **!range | range**
  Specifies the range criteria.
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  *start_range* must be an integer from 1 through 65535.
  *end_range* must be an integer from 1 through 65535, and must be greater than *start_range*.

- **port-map port_map**
  Specifies name of the port-map for the port range.
  *port_map* must be a string of 1 through 63 characters in length.

Usage
Use this command to specify an access/firewall ruledef to analyze user traffic based on destination UDP port.

Example
The following command creates an access/firewall ruledef for analyzing user traffic matching destination port for UDP as 10:

```
udp dst-port = 10
```
udp either-port

This command configures an access/firewall ruledef to analyze user traffic based on either (destination or source) UDP port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] udp either-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } } }  

no
Removes previously configured either-port (destination or source) UDP ruledef.

operator
Specifies how to logically match the port number.
operator must be one of the following:

• !=: Does not equal
• <=: Less than or equals
• =: Equals
• >=: Greater than or equals

port_number
Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range
Specifies the range criteria.

• !range: Not in the range
• range: In the range

start_range to end_range
Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535, and must be greater than start_range.

port-map port_map
Specifies name of the port-map for the port range.
port_map must be a string of 1 through 63 characters in length.
Usage
Use this command to specify an access/firewall ruledef to analyze user traffic based on either UDP port.

Example
The following command creates an access/firewall ruledef for analyzing user traffic matching destination or source port for UDP as 10:

```
udp either-port = 10
```
udp src-port

This command configures an access/firewall ruledef to analyze user traffic based on source UDP port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] udp src-port { operator port_number | { !range | range } { start_range to end_range } | port-map port_map } }
```

- **no**
  Removes previously configured source UDP port ruledef.

- **operator**
  Specifies how to logically match the port number.
  - `!`: Not equal
  - `<`: Less than or equals
  - `=`: Equals
  - `>`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  - `port_number` must be an integer from 1 through 65535.

- **!range | range**
  Specifies the range criteria.
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  - `start_range` must be an integer from 1 through 65535.
  - `end_range` must be an integer from 1 through 65535, and must be greater than `start_range`.

- **port-map port_map**
  Specifies name of the port-map for the port range.
  - `port_map` must be a string of 1 through 63 characters in length.

Usage
Use this command to specify an access/firewall ruledef to analyze user traffic based on source UDP port.

**Example**
The following command creates an access/firewall ruledef for analyzing user traffic matching source port for UDP as 10:

```plaintext
udp src-port = 10
```
Chapter 101
FTP Configuration Mode Commands

The FTP Configuration Mode is used to manage the FTP server options for the current context.

- Exec Mode
  - configure
    - Global Configuration Mode
      - context name
        - Context Configuration Mode
          - server ftpd
            - FTP Configuration Mode
end

Exits the FTP server configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
end
```

Usage
Change the mode back to the Exec mode.
exit

Exits the FTP server configuration mode and returns to the context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the context configuration mode.
max servers

Configures the maximum number of FTP servers that can be started within any 60 second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
max servers count
```

```
count
Default: 40
Specifies the maximum number of servers that can be spawned in any 60 second interval. count must be a value in the range from 1 to 100.
```

Usage
Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that FTP services do not cause excessive system impact to other services.

Example
```
max servers 50
```
timeout

Configures the client idle timeout before an FTP session is automatically closed.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
timeout seconds
```

- `seconds`
  - Default: 900
  - Specifies the number of seconds of inactivity before an FTP session is automatically closed. `seconds` must be in the range from 10 through 86400.

**Usage**
Adjust the session timeout to fine tune the system. FTP session resources can be released sooner to support additional requests by adjusting the timeout to a smaller value.

**Example**
```
timeout 300
```
Chapter 102
GGSN Service Configuration Mode Commands

The Gateway GPRS Support Node (GGSN) Configuration Mode is used to create and manage GGSN services within the current context.

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

Configures the name of the context configured on the system that processes accounting for PDP contexts handled by this GGSN service.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
accounting context context_name
no accounting context
```

**no**
Removes a previously configured accounting context.

**context_name**
Specifies the name of the context to be used for accounting. The name must be between 1 and 79 alpha and/or numeric characters and is case sensitive.

**Usage**
By default, the system attempts to use the same context as the one in which the GGSN service is configured for accounting purposes. This command can be used to either change the system’s default behavior, or allow GPRS Tunneling Protocol Prime (GTPP) accounting to a charging gateway (CG).

By default when GTPP accounting is used, accounting records will be sent to the accounting servers configured in whichever context the GGSN service is configured. This command may be used to override that default.

**Example**
The following command configures the GGSN service’s accounting context to be plmn1:

```plaintext
accounting context plmn1
```
**authorize-with-hss**

This command enables/disables subscriber session authorization with HSS over S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[default] authorize-with-hss
```

**Usage**
Use this command to enable/disable the authorization support for subscriber over S6b interface which is used between GGSN and the 3GPP AAA to exchange the information related to charging, P-CSCF discovery, etc. By use of this feature allows the GGSN service to interact with HSS over S6b interface through Diameter configuration which is already configured on the system.

**Important:** Diameter configuration must be available before enabling this command. For more information of Diameter interface configuration, refer Diameter Endpoint Configuration Mode Commands chapter.

**Important:** This command is a license-enabled feature.

**Example**
The following command enables the subscriber authorization with HSS over S6b Diameter interface to provide session interoperability between GGSN and PGW and HA in this GGSN service:

```
authorize-with-hss
```
bind

Binds the GGSN service to a logical IP interface serving as the Gn interface. Specifies the maximum number of subscribers that can access this service over the interface.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bind address address [max-total-pdp-contexts max_total | max-ppp-pdp-contexts max_ppp]
```

```
no bind address address
```

**no**
Removes a previously configured binding for the GGSN service.

**address**
Specifies the IP address (address) of the interface configured as the Gn interface. address is specified in dotted decimal notation.

**max-total-pdp-contexts max_total**
Default: 1,500,000
Specifies the maximum number of PDP contexts (both IP and PPP) that can access this service on this interface.

**max-ppp-pdp-contexts max_ppp**
Default: 750,000
Specifies the maximum number of PPP PDP contexts that can access this service on this interface.

**Important:** The maximum number of subscriber contexts supported is dependant on the session capacity license installed and the number of active PACs/PSCs installed in the system. A fully loaded ASR 5000 with 13 active PSCs can support 4,000,000 total IP and PPP PDP contexts. Note that each PPP PDP context is treated as two IP PDP contexts. Refer to the license key command for additional information.

**Important:** The maximum number of subscriber contexts supported is dependant on the session capacity license installed and the number of active PACs installed in the system. A fully loaded ST16 system with 13 active PACs can support 1,500,000 PPP PDP contexts. Refer to the license key command for additional information.

**Important:** The maximum number of subscriber contexts supported is dependant on the session capacity license installed and the number of active processing cards installed in the system. A fully loaded ASR 5000 with 13 active PACs can support 1,500,000 PPP PDP contexts. Refer to the license key command for additional information.
processing cards can support 2,500,000 total PPP PDP contexts. Refer to the license key command for additional information.

Usage

Used to associate or tie the GGSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Gn interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a “soft” limit as to the number of simultaneous subscriber contexts that can be facilitated by the service/interface at any given time. Soft limits are based on measurements gathered at regular short intervals (several times per minute) as opposed to measurements taken in real-time. Therefore the sampled measurement may not match the actual number of PDP contexts currently being processed. Every PDP context request received is compared against the result of the last sample. If the sample is less than the soft limit configured, the request will be processed. If it is more, the request will be rejected.

When configuring the max-total-pdp-contexts or max-ppp-pdp-contexts options, be sure to consider the following:

- Each PPP PDP context is treated as two IP PDP contexts due to the additional CPU and memory resources required
- The total number of interfaces that you configure for use as Gn interfaces
- The maximum number of subscriber PDP contexts that all of the interfaces may handle during peak busy hours
- The average bandwidth for each of the PDP contexts
- The type of physical port (10/100Base-T or 1000Base-Tx) to which these interfaces are bound

Taking these factors into account and distributing your subscriber contexts across all available interfaces allows you to configure your interfaces to optimally handle PDP contexts without degraded performance.

Example

The following command would bind the logical IP interface with the address of 192.168.3.1 to the GGSN service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```
cc behavior

Configures the 3GPP behavior bits associated with the GGSN’s charging characteristics (CC).

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

cc behavior no-records nr_value }

no-records nr_value
Default: 0 (disabled)
Specifies the behavior bit upon which the GGSN ceases sending accounting records to a server.
nr_value can be configured to any integer value between 1 and 12 corresponding to the 12 behavior bits B1 through B12.

Usage
3GPP standards after 3GPP R98 included 12 behavior bits as part of GGSN charging characteristics. Like the charging characteristics profile index, the behavior bits are sent by the SGSN to the GGSN in the Create PDP Context request message.
This command configures the behavior bits for each of the conditions described.

Example

The following command configures a behavior bit of 10 for no-records:

cc behavior no-records 10
**cc profile**

Configures the charging characteristic (CC) profile index properties.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cce profile index [bucket number | interval time [downlink down_octets uplink up_octets | total total_octets ] | prepaid {prohibited | use-rulebase-configuration } | server address context | sgsns num_changes | tariff time1 mins hours [time2 mins hours [time3 mins hours [time4 mins hours [time5 mins hours [time6 mins hours ]]]] | volume {downlink vol_down_octets uplink vol_up_octets | total total_octets } ]
```

```
no cc profile index {bucket | interval | prepaid | server address | sgsns | tariff | volume }
```

```
default cc profile index [bucket | interval | prepaid | server address | sgsns | tariff | volume]
```

---

**no**

Removes a previously configured profile index.

**default**

Returns the specified cc profile to the original default system settings.

**index**

Configures a profile index for the parameter to be specified. index can be configured to any integer value from 0 to 15.

---

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

```
buckets number
```

Default: 4

Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.

*number* can be configured to any integer value from 1 through 4.
interval time [downlink down_octets uplink up_octets | total total_octets ]

Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions occur:

- Downlink traffic volume is reached within the time interval
- Uplink traffic volume is reached within the time interval
- Total traffic volume (up and downlink) is reached within the time interval

time is measured in seconds and can be configured to any integer value from 60 to 40,000,000.
down_octets is the downlink traffic volume measured in octets and can be configured to any integer value from 0 to 1,000,000.
up_octets is the uplink traffic volume measured in octets and can be configured to any integer value from 0 to 1,000,000.
total_octets is the total traffic volume measured in octets and can be configured to any integer value from 0 to 1,000,000.

prepaid {prohibited | use-rulebase-configuration }

This command enables or disables prepaid for the specified profile index.
Default: N/A
prohibited: Disable prepaid for the specified profile index.
use-rulebase-configuration: Use the prepaid configuration in the rulebase.

sgsns num_changes

Default: 4
Specifies the number of SGSN changes (i.e., inter-SGSN switchovers) resulting in a new RAI (Routing Area Identity) that can occur before closing an accounting record.
um_changes can be configured to any integer value from 1 to 15.

tariff time1 mins hours time2 mins hours time3 mins hours time4 mins hours time5 mins hours time6 mins hours

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.

Important: The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:
- mins: The minutes of the hour, an integer value from 0 to 59.
- hours: The hour of the day, an integer value from 0 to 23.

volume {downlink vol_down_octets uplink vol_up_octets | total total_octets }

Specifies the downlink, uplink, and total volumes that must be met before closing an accounting record.
vol_down_octets is measured in octets and can be configured to any integer value from 100,000 to 4,000,000,000.
vol_up_octets is measured in octets and can be configured to any integer value from 100,000 to 4,000,000,000.
**total_octets** is the total traffic volume (up and downlink) measured in octets and can be configured to any integer value from 100,000 to 4,000,000,000.

**Usage**

Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the GGSN’s charging characteristics. The GGSN supports up to 16 profile indexes. This command works in conjunction with the cc-sgsn command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts.

**Example**

The following command configures a profile index of 10 for tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10 tariff time1 0 7 time2 30 19 time3 0 7 time4 30 19
```
**default**

Sets/restores the default value assigned for the specified parameter.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
default {cc {behavior | profile index } | echo-interval | gtpu echo-interval | gtpu reorder {context | sequence-numbers | timeout } | guard-interval | ip {local-port gtpc-v1 | qos-dscp } | max-retransmissions | plmn {unlisted-sgsn } | setup-timeout | timeout }
```

```
cc {behavior | profile index }
```

Restores the GGSN’s charging characteristics parameters to the following default settings:
- **behavior**: Restores all behavior parameters to their default values of 0 (disabled).
- **profile**: For the specified index, the following defaults are applied:
  - buckets: 4
  - interval: Disabled
  - volume: Disabled
  - sgsns: 4
  - tariff-time: Disabled

```
echo-interval
```

Restores the GTP echo-interval parameter to its default setting of 60.

```
gtpu echo-interval
```

Restores the GTPU echo-interval parameter to its default setting of 60.

```
gtpu reorder {context | sequence-numbers | timeout }
```

Restores the gtpu reordering parameters to the following default settings:
- gtpu reorder context: Disabled
- gtpu reorder sequence-numbers: Disabled
- gtpu reorder timeout: 100 milliseconds

```
gtpu udp-checksum insert
```

Restores the GGSN gtpu udp-checksum parameter to its default setting of enabled.

```
guard-interval
```

Restores the GGSN guard-interval parameter to its default setting of 100.
ip {local-port gtpc-v1 | qos-dscp }
Restores the GGSN ip parameters to the following default setting:
- **local-port gtpc-v1**: 2123
- **qos-dscp**: conversational ef streaming af11 interactive af21 background be

max-retransmissions
Restores the GGSN max-retransmissions parameter to its default setting of 4.

plmn {unlisted-sgsn }
Restores the GGSN plmn unlisted-ggsn parameter to its default setting of reject.

setup-timeout
Restores the GGSN setup-timeout parameter to its default setting of 60.

timeout
Restores the GGSN timeout parameter to its default setting of 5.

Usage
After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

Example
The following command restores the GGSN service’s guard interval parameter to its default setting:

default guard-interval
dns-client

This command defines the context name where a DNS client is configured. This command will associates an existing DNS client configuration with GGSN to perform DNS query for P-CSCF, if P-CSCF query request in AAA message is received from Diameter node.

Product
All

Privilege
Security Administrator, Administrator

Syntax

dns-client context dns_ctxt_name

[no] dns-client context

no
Removes the association of DNS context which was configured to perform DSN query in this GGSN service.

dns_ctxt_name
Specifies the name of the context in which a DNS client configuration is present. Typically this should be the same where this GGSN service is configured.
dns_ctxt_name is a context name and must be alpha and/or numeric string of 1 through 79 characters.

Usage
Use this command to associate a DNS client configuration to perform DNS query used for the resolution of P-CSCF query received in AAA message from Diameter peer, on the basis of DNS client parameters configured in a context.
A DNS client configuration must be present in the same context as GGSN service before enabling this command to perform DNS query for P-CSCF.

Important: This command is a license-enabled feature.

Example
The following command associates a DNS client configuration to perform DNS query for P-CSCF with this GGSN service which is configured in same context as GGSN service:

default dns-client context
**echo-interval**

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-C Echo packets are sent from the GGSN service to the SGSN.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
echo-interval time_interval
no echo-interval
```

- **time_interval**
  
  Default: 60
  
  Specifies the frequency at which the GGSN service sends GTPv1-C Echo packets to the SGSN(s) it is configured to communicate with.
  
  `time_interval` is measured in seconds and can be configured to any integer value between 60 and 3600.

**Usage**

Use this command to adjust the rate at which the GGSN sends these packets. GTPv1-C Echo packets are used to detect whether SGSNs that the GGSN service is communicating with, has become unresponsive or has rebooted.

The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new SGSN on the system using the `sgsn address` command as described in this chapter
- Upon the execution of the path failure detection policy as described in the `path-failure` command of this chapter

The echo-interval command is used in conjunction with the `max-retransmissions` and `retransmission-timeout` commands as described in this chapter.

In addition to receiving an echo response for this echo protocol, if GGSN receives a Node Alive Request message or a Echo Request message from a presumed dead SGSN, it will immediately assume the SGSN is active again.

If the GGSN discovers that an SGSN has become unresponsive, it will terminate all PDP contexts that had been established with the SGSN.

**Example**

The following command configures the GGSN service to send GTP Echo packets every 120 seconds:
echo-interval 120
end

Exits the GGSN service configuration mode and returns to the Administrator-Exec mode prompt.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Administrator-Exec mode.
exit

Exits the GGSN service configuration mode and returns to the context configuration mode.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Returns to the context configuration mode.
fqdn

This command defines Fully Qualified Domain Name (FQDN) which would be used for authorization over S6b interface between GGSN and 3GPP AAA/HSS.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[no | default] fqdn host host_name realm realm_id

no
Removes configured FQDN host name and realm id from GGSN service.

default
Sets the system to default mode for this command and configure the host and realm id value to NULL.

host host_name
Specifies the name of the host to be used for authorization over S6b interface with 3GPP AAA server/HSS from GGSN service. host_name is a unique name that need to be configured for the authorization over S6b interface from this GGSN service. host_name must be an alpha and/or numeric string of from 1 through 127 characters. host_name allows punctuation marks.

realm realm_id
Specifies the realm as FQDN to be used for authorization over S6b interface with 3GPP AAA server/HSS from GGSN service. The realm may typically be a company or service name. realm_id is a unique identifier that need to be configured for the authorization over S6b interface from this GGSN service and must be an alpha and/or numeric string of from 1 through 127 characters. It allows punctuation marks. host_name

Usage
Use this command to define host and realm as FQDN for 3GPP AAA server/HSS which would be used for authorization over S6b interface with GGSN. The realm specified as FQDN may typically be a company or service name.
By default the FQDN host and realm will be NULL

Important: This command is a license-enabled feature.

Example
The following configures the `hss1` as host name and `xyz.com` as realm for FQDN to support authorization over S6b from this GGSN service:

```
fqdn host hss1 realm xyz.com
```
gtpc nsapi-in-create-pdp-response

This command configures the exclusion/inclusion of optional information element (IE) Network Service Access Point Identifier (NSAPI) in “Create PDP Context Response” messages in GTP-C.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

[default | no] gtpc nsapi-in-create-pdp-response

default
Sets the default mode for GTP-C messages; i.e. to not to include NSAPI IE in “Create PDP Context Response” messages.

no
Removes the preconfigured mode for GTP-C messages; in other words sets the mode for GTP-C message to not to include NSAPI IE in “Create PDP Context Response” messages. By default it is disabled.

Usage
Use this command to configure the mode for the GTP-C messages to exclude or include the NSAPI IE in “Create PDP Context Response” message received from SGSN.

Example
The following command configures the GGSN service to include the optional IE of NSAPI in “Create PDP Context Response” message:

gtpc nsapi-in-create-pdp-response
**gtpc private-extension**

This command configures the customer specific private extension in GTP-C messages.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpc private-extension {{focs | odb} access-list acl_name in disconnect-on-violation } | ggsn-preservation-mode | insk | loss-of-radio-coverage | none}
default gtpc private-extension

no gtpc private-extension [focs | insk | preservation-mode | loss-of-radio-coverage]
```

**default**
Sets the default mode for GTP-C messages. By default it is disabled.

**no**
Disables the configured private extensions for GTP-C messages.

```
{focs | odb} access-list acl_name in disconnect-on-violation
```

These keywords configures the Free-Of-Charge-Service and Operator Determined Barring for all packet oriented services as defined by operators.

**focs**: This keyword enables/disables Free of Charging Services for the subscriber who has no credit, and also takes the access-list `acl_name` to be applied for FOCS.

**odb**: This keyword enables/disables “all packet oriented service barred” for the subscriber, and also takes the access-list `acl_name` to be applied for ODB.

`acl_name` is the name of configured access control list for this service.

**Important**: These are the customer-specific keywords and need customer-specific license to use them.

```
insk
```

This keyword is for the Intelligent-Network-Service-Key defined by vendors. This private extension can be present in Create PDP Context request messages.

A radius dictionary can be configured to send that value in accounting messages.

**Important**: This is a customer specific-keyword and needs customer-specific license to use this feature.
gtpc private-extension

**ggsn-preservation-mode**

This keyword is the customer specific option and used to indicate the presence of such a private extension in Update PDP Context requests. It indicates whether the subscriber is active or has become idle, and RAN resources might have been released. It also indicates the "type" of desired preservation mode behavior. System support two different types of behavior. When **ggsn-preservation-mode** is configured, different generation of accounting records occur based on the "type" of mode. To enable the different generation of accounting records, the trigger for preservation mode must be configured for RADIUS or GTPP command for that accounting protocol. If that trigger is not configured, there will be no change in the generation of accounting records.

**Important:** This is a customer-specific keyword and needs customer-specific license to use this feature.

**loss-of-radio-coverage**

These keywords enables the protection for overcharging to a subscriber due to loss of radio coverage (LORC) in a GGSN service. It also enables the system to understand the private extension in GTP-C message for LORC in Update PDP Context message from SGSN.

**Important:** This is a license enabled keyword and need feature-specific license to use it.

**none**

Removes the private extensions from record which are from GTP-C messages received from the SGSN.

**Usage**

Use this command to configure the private extensions to record from the GTP-C messages received from SGSN. It also configures the customer specific features; i.e. preservation mode for GGSN service. Overcharging protection for LORC is a solution which provides the ability to configure mobile carriers to maximize their network solutions and balancing the requirements to accurately bill their customer.

Consider scenario where a mobile is streaming or downloading very large files from external sources and the mobile goes out of radio coverage. If this download is happening on Background/Interactive traffic class then the GGSN is unaware of such loss of connectivity as SGSN does not perform the Update PDP Context procedure to set QoS to 0kbps (this is done when traffic class is either Streaming or Conversational only). The GGSN continues to forward the downlink packets to SGSN. In the loss of radio coverage, the SGSN will do paging request and find out that the mobile is not responding; SGSN will then drops the packets. In such cases, the G-CDR will have increased counts but S-CDR will not. This means that when operators charge the subscribers based on G-CDR the subscribers may be overcharged. This feature is implemented to avoid the overcharging in such cases.

This implementation is based on Cisco-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.

**Important:** This is a license enabled command and needs feature-specific license/s to use this command.

**Important:** Some of the keywords a customer-specific feature and need customer-specific license/s to use them.

**Example**
The following command configures the GGSN service to record the private extension for intelligent network service key as defined by operator:

```
gtpc private-extension insk
```
**gtpc ran-procedure-ready-delay**

This command configures the GGSN to enable the RAN Procedure Ready feature for the particular GGSN service and specify the timeout period for RAN procedure timer in GGSN which is started on arrival of every secondary Create PDP Context request.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
gtpc ran-procedure-ready-delay [timeout dur]
```

- **default**
  
  Sets the default mode of RAN Procedure Ready feature for the particular GGSN service. By default it is disabled.

- **no**
  
  This keyword is used to disable RAN Procedure Ready feature for the particular GGSN service. By default it is disabled.

- **timeout dur**

  Default: 10
  
  Specifies the timeout duration in seconds for RAN procedure timer in GGSN which is started on arrival of every secondary “Create PDP Context Request” message.
  
  This is an optional keyword. If no timeout period is specified then default value of 10 seconds will be assigned to timeout period.
  
  *dur* must be an integer between 1 through 40.

**Usage**

Use this command to enable the RAN Procedure Ready feature for the particular GGSN service and to specify the timeout period for RAN procedure timer in GGSN which is started on arrival of every secondary “Create PDP Context Request” message.

Once a “Create PDP Context Request” is received by GGSN from SGSN, a timer will be started at GGSN and GGSN will wait till the Radio Access Bearer setup is completed and “Update PDP Context Request” is sent by SGSN. If any downlink data is received before arrival of “Update PDP Context Request” or before timer expire, that downlink packets will be queued or buffered. Currently buffer limit of sub-system is 1024 packets.

To support this feature each sub-session uses a common flag ‘ran procedure ready state’, whenever a “Create PDP Context Request” is received for secondary PDP context and sub-session is allocated, this flag will be set to TRUE by default. This common flag is checked while sending downlink traffic, if this flag is FALSE then GGSN permit flow of downlink data but, if it is TRUE, GGSN will queue the downlink packets.

In case if the buffer becomes full (total buffer limit is of 1024 packets) then, all the newly coming packets will be dropped.
If “Update PDP Context Request” is received by GGSN with RAN Procedure flag set or if timer expires the 'ran-procedure ready state' flag in sub-session will be reset and hence GGSN will start sending queued packets in ‘first-in first-out’ manner and buffering will be disabled for further downlink traffic.

This feature supports following scenarios when RAB setup timer starts at the GGSN:

- If GGSN receives the “Update PDP Context Request” before timer expires, with RAN Procedure Ready bit TRUE (1), then GGSN will stop the timer, send all the queued/buffered packets in ‘first-in first-out’ manner and change the ‘ran procedure ready state’ to FALSE and disables buffering of further downlink data.

- If GGSN receives the “Update PDP Context Request” before timer expires, with RAN Procedure Ready bit FALSE (0), then GGSN will process the “Update PDP Context Request” as usual, but will not disable the buffering of downlink data and wait for other “Update PDP Context Request” to come with RAN procedure ready flag set or wait for timer to expire.

- If GGSN do not receive the “Update PDP Context Request” with RAN Procedure Ready bit TRUE (1) before timer expire, the timer will be fired and GGSN starts sending all the queued packet and will change the ‘ran procedure ready state’ to FALSE and disables buffering of further downlink data (assuming that the corresponding SGSN does not support this feature).

- If timer has expired and GGSN received an “Update PDP Context Request” for secondary PDP context with or without RAN Procedure Ready bit set, the UPC will be processed as usual without making any changes for buffering the packets.

**Important**: This feature make no effect on Enhanced Charging Service or DPI as the buffering of downlink data is done before sending it to ACSMgr.

**Important**: During SGSN handoff scenario all packets will be processed in a normal way and the downlink packets buffered till the timer expires.

**Example**
The following command configures the GGSN service to enable the RAN Procedure Ready feature and specify the timeout period as 20 seconds for RAN procedure timer in GGSN:

```
gtpc ran-procedure-ready-delay timeout 20
```
gtpu echo-interval

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-U Echo packets are sent from the GGSN service to the SGSN.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpu echo-interval time_interval
no gtpu echo-interval
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the sending of GTPv1-U Echo packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>time_interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 60</td>
</tr>
<tr>
<td>Specifies the frequency at which the GGSN service sends GTPv1-C Echo packets to the SGSN(s) it is configured to communicate with.</td>
</tr>
<tr>
<td>time_interval is measured in seconds and can be configured to any integer value between 60 and 3600.</td>
</tr>
</tbody>
</table>

Usage
GTPv1-C Echo packets are used to detect whether SGSNs that the GGSN service is communicating with, has become unresponsive or has rebooted. Use this command to adjust the rate at which the GGSN sends these packets.
If the GGSN discovers that an SGSN has become unresponsive, it will terminate all PDP contexts that had been established with the SGSN.

Example
The following command configures the GGSN service to send GTPv1-U Echo packets every 120 seconds:

```
gtpu echo-interval 120
```
**gtpu reorder**

Configures packet data reordering for the GGSN service.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpu reorder {context {ppp } | sequence-numbers {ipv4 | ppp | ipv4-ppp | ppp-ipv4 } | timeout time }

no gtpu reorder {context | sequence-numbers {ipv4 | ppp | ipv4-ppp | ppp-ipv4 } }
```

**no**
Disables the re-ordering of GTPU packets.

**context {ppp }**
Default: Disabled
Enables the GGSN service to re-order PPP data packets based on the sequence numbers inserted by the SGSN.

**sequence-numbers {ipv4 | ppp | ipv4-ppp | ppp-ipv4 }**
Default: Disabled
Enables the GGSN service to insert sequence numbers into the data packets that it sends to the SGSN.
The insertion of sequence numbers can be controlled for specific PDP context types. The following PDP context types can be specified:

- **ipv4**: Enables re-ordering for IP PDP context types
- **ppp**: Enables re-ordering for PPP PDP context types
- **ipv4-ppp**: Enables re-ordering for both IP and PDP context types
- **ppp-ipv4**: The same as ipv4-ppp, enables re-ordering for both IP and PDP context types

**Important**: If packet re-ordering is enabled using the `gtpu reorder context` command, sequence numbers are automatically be added regardless of this command.

**timeout time**
Default: 100 milliseconds
If re-ordering is enabled, this option specifies the amount of time that the GGSN should wait prior to sending re-sequenced data packets stored in queue.

- time is measured in milliseconds and can be configured to any integer value between 0 and 5000. A timeout of “0” indicates that only packets arriving in sequence are processed and the accepted sequence number is updated for each in-sequence packet. Packets are not queued. Packets arriving with seq number less than the accepted sequence number are discarded.
Usage
Use this command to control data packet re-ordering between the GGSN and SGSN. If re-ordering is enabled for the GGSN service, the GGSN informs the SGSN to also reorder the data packets from the GGSN. The GGSN informs the SGSN in the create PDP context response. The GGSN and SGSN optionally insert sequence numbers into the data packets that they send.

Example
The following command specifies that the GGSN service re-sequences data packets received from the SGSN for PPP PDP context types:

    gtpu reorder context ppp

The following command specifies that the GGSN service inserts sequence numbers for both IP and PPP PDP context types into data packets it is sending to the SGSN for PPP PDP context types:

    gtpu reorder sequence-numbers ppp-ipv4
gtpu udp-checksum insert

This command enables/disables the insertion of UDP checksum in outgoing UDP data packets. By default checksum insertion is enabled.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no | default] gtpu udp-checksum insert
```

- **no**
  Disables insertion of UDP checksum in outgoing UDP data packets.

- **default**
  Enables the insertion of UDP checksum in outgoing UDP data packets.

**Usage**

Use this command to enable or disable the system to insert UDP checksum in outgoing UDP data packets.

**Example**

The following command specifies that the GGSN service will insert the UDP checksum into outgoing UDP data packets:

```
gtpu udp-checksum insert
```
guard-interval

Configures the time period after which a redundant PDP context request received from an SGSN is treated as a new request rather than a re-send of a previous request.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
guard-interval guard_time
no guard-interval
```

**no**
Disables the guard-interval function for the GGSN service.

**guard_time**
Default: 100
Specifies the amount of time that must pass before a GGSN service treats a redundant PDP context request as a new request instead of a re-send of a previous request.

*guard_time* is measured in seconds and can be configured to any integer value between 10 and 3600.

Usage
The guard interval is used to protect against replay attacks. Without a guard interval configured, information from a valid PDP context request could be used to gain un-authorized network access.

If the GGSN service receives a PDP context request in which the International Mobile Subscriber Identity (IMSI), the Network Service Access Point Identifier (NSAPI), the end user IP address, and the GTP sequence number are identical to those received in a previous request, the GGSN treats the new request as a re-send of the original. Therefore, information from a valid PDP context request could be collected and re-sent at a later time by an un-authorized user to gain network access.

Configuring a guard interval limits the amount of time that the information contained within a PDP context request remains valid.

Example
The following command configures the GGSN service with a guard interval of 60 seconds:

```
guard-interval 60
```
**ip local-port**

Configures the local User Datagram Protocol (UDP) port for the Gn interfaces’ GTPC socket for GTPv1.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip local-port gtpc-v1 port#
```

**gtpc-v1 port#**

Default: 2123

Specifies the UDP port number for GTPv1 GTPC sockets.

`port#` can be configured to any integer value between 1 and 65535.

**Usage**

By default, the GGSN service attempts to use GTPv1 when communicating with SGSNs. This parameter configures the UDP port over which the GTP control (GTPC) sockets are sent. If an SGSN only supports GTPv0, the GGSN service automatically switches to GTPv0 when communicating with this SGSN. In the scenario, the GGSN service communicates with the SGSN on UDP port 3386 and does not have a GTPC socket.

**Important:** The UDP port setting on the SGSN must match the local-port setting for the GGSN service on the system in order for the two devices to communicate.

**Example**
The following command configures the GGSN service to use UDP port 2500 for exchanging GTPC sockets with SGSNs when using GTPv1:

```
ip local port 2500
```
ip qos-dscp

Configures the quality of service (QOS) differentiated service code point (DSCP) used when sending data packets over the Gn interface.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

\[
\text{ip qos-dscp \{\{allocation-retention-priority | background | conversational | interactive traffic_priority | streaming \} \{ dscp\}\}+}
\]

\[
\text{no ip qos-dscp \{allocation-retention-priority | background | conversational | interactive traffic_priority | streaming\} +}
\]

\textbf{allocation-retention-priority}

Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile. \textit{allocation-retention-priority} can be the integers 1, 2, or 3. DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile. The following table shows the DSCP value matrix for \textit{allocation-retention-priority}.

\begin{table}
\centering
\begin{tabular}{|c|c|c|c|}
\hline
\textbf{Allocation Priority} & 1 & 2 & 3 \\
\hline
\textbf{Traffic Handling Priority} & ef & ef & ef \\
\hline
1 & af21 & af21 & af21 \\
\hline
2 & af21 & af21 & af21 \\
\hline
3 & af21 & af21 & af21 \\
\hline
\end{tabular}
\end{table}

\textbf{background}

Specifies the QOS for traffic patterns in which the data transfer is not time-critical (for example email exchange). This traffic pattern requires the lowest QOS.

\textbf{conversational}

Specifies the QOS for traffic patterns in which there is an constant flow of packets in each direction, upstream and downstream. This traffic pattern requires the highest QOS.
**interactive**

Specifies the QOS for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. This traffic pattern requires a higher QOS than the background pattern, but not as high as that for the streaming pattern.

*traffic_priority* is the 3GPP traffic handling priority and can be the integers 1, 2 or 3.

**streaming**

Specifies the QOS for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream. This traffic pattern requires a higher QOS than the interactive pattern, but not as high as that for the conversational pattern.

**dscp**

Default:

- background: be
- interactive:
- Traffic Priority 1: ef
- Traffic Priority 1: af21
- Traffic Priority 1: af21
- streaming: af11
- conversational: ef

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

- **af11**: Assured Forwarding 11 per-hop-behavior (PHB)
- **af12**: Assured Forwarding 12 PHB
- **af13**: Assured Forwarding 13 PHB
- **af21**: Assured Forwarding 21 PHB
- **af22**: Assured Forwarding 22 PHB
- **af23**: Assured Forwarding 23 PHB
- **af31**: Assured Forwarding 31 PHB
- **af32**: Assured Forwarding 32 PHB
- **af33**: Assured Forwarding 33 PHB
- **af41**: Assured Forwarding 41 PHB
- **af42**: Assured Forwarding 42 PHB
- **af43**: Assured Forwarding 43 PHB
- **be**: Best effort forwarding PHB
- **ef**: Expedited forwarding PHB

More than one of the above keywords can be entered within a single command.

**Usage**

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they’re tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.
The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

**Table 22. Class structure for assured forwarding (af) levels**

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

**Table 23. DSCP Precedence**

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>1</td>
<td>Class 1</td>
</tr>
<tr>
<td>2</td>
<td>Class 2</td>
</tr>
<tr>
<td>3</td>
<td>Class 3</td>
</tr>
<tr>
<td>4</td>
<td>Class 4</td>
</tr>
<tr>
<td>5</td>
<td>Express Forwarding (ef)</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command. The no ip qos command can be issued to remove a QOS setting and return it to it’s default setting.

**Example**

The following command configures the DSCP level for the streaming traffic pattern to be ef:

```
ip qos streaming ef
```

The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be ef, ef, af22, and af41, respectively:

```
ip qos-dscp conversational ef streaming ef interactive af22 background af41
```
max-retransmissions

Configures the maximum number of times that GTP control packets are retransmitted to an SGSN before it marks it unreachable.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax
max-retransmissions max_number

max_number
Default: 4
Indicates the maximum number of times that GTP control packets are retransmitted.
max_number can be configured to any integer value between 0 and 15.

Usage
This command is used in conjunction with the timeout command to control the retransmission of GTP control packets when no response is received from an SGSN. It is equivalent to the N3-REQUESTS parameter discussed in 3GPP TS 29.060.
If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of this command.
If the max-retransmissions value is exceeded, the GGSN records a “Path Failure” for that SGSN and releases all PDP contexts associated with it.

Example
The following command configures the maximum number of retransmissions to 8:

max-retransmissions 8
mbms policy

This command enables/disables the MBMS user service support for Multicast and/or Broadcast mode. It also specifies the policy for MBMS user service mode.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
mbms policy multicast broadcast
[no | default] mbms policy
```

- **no**
  Removes/disables the configured MBMS support for Multicast and/or Broadcast mode in this GGSN service.

- **default**
  Restores the default mode of MBMS support in this GGSN service.

- **multicast broadcast**
  Enables the MBMS support and configures the policy for multicast and broadcast of user service.

**Usage**
Use this command to enable/disable the MBMS user service support for Multicast and/or Broadcast mode. It also specifies the policy for MBMS user service mode.

**Example**
The following command enables the MBMS support in this GGSN service:

```plaintext
mbms policy multicast broadcast
```
**newcall**

This command enables/disables the new call related behavior of GGSN service when duplicate sessions with same IP address request is received. This feature is required to support the interworking with P-GW and HA.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[default] newcall duplicate-subscriber-requested-address {accept | reject}
```

**default**

Restores the default mode for new call session with same address request received in this GGSN service. It sets the new call related behavior to reject call with duplicate address request.

**accept**

Sets the system to “accept” the another session using same IP address for new call. New session will be accepted and old session will be torn down.

Default: Disbaled

**reject**

Reject new call with duplicate address request. This is the default behavior.

Default: Enabled

**Usage**

Use this command to enable/disable to support the new connection where UE is not able to gracefully disconnect from the Enterprise PDN before it attempts to reconnect via another access method. The Enterprise xGW (GGSN) shall be able to tear down the old session in order to accept the new connection with the same IP address assignment.

By use of this feature GGSN will allow accepting request for static subscriber address, even if address is already used by another session. If this feature is not enabled, then new request with same IP address for another session will be rejected.

**Important:** This command is a license-enabled feature.

**Example**

The following command allows the GGSN to accept the duplicate call session request with same IP address:

```
newcall duplicate-subscriber-requested-address accept
```
path-failure

Determines the GTP path-failure behavior on echo/non-echo messages.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

path-failure detection-policy gtp {echo [non-echo] | non-echo [echo] }

[no | default] path-failure detection-policy

| no |
| No defined detection policy means path-failures are not detected. |

| default |
| Use the default command to set the path-failure detection-policy to gtp in echo mode. |

| detection-policy gtp {echo [non-echo] | non-echo [echo] } |
| Detection-policy is the policy to be used when path-failure is in the default active state. GTP messages are either gtp(u) (user) or gtp(c) (control) type, and the gtp keyword takes either echo or non-echo as message type. |
| echo: gtp(u) or gtp(c) message. |
| non-echo: a message type other than gtp(u) or gtp(c). |

Usage

Under current circumstances, a GGSN shuts down the GTP tunnel if the associated SGSN does not respond to multiple retries of an echo or non-echo message from the GGSN. In this way, a single call failure could be responsible for the loss of all active calls in the tunnel.
This is also an issue when echo is disabled, or when there is very little traffic on the SGSN and the GGSN is configured with large echo intervals.
This behavior adversely impacts the user experience because the customer has to reconnect every time this happens with their SGSN.

Example

The following example detects path failures when the SGSN fails to respond to multiple echo message retries:

```
path-failure detection-policy gtp echo
```

The following example turns off path-failure detection. On timeout of gtp(c) message retries, the particular context will be purged:

```
no path-failure detection-policy
```
plmn id

Configures the GGSN’s public land mobile network (PLMN) identifiers. Up to five PLMN IDs can be configured for each GGSN service.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

plmn id mcc mcc_number mnc mnc_number [primary]
o plmn id mcc mcc_number mnc mnc_number

no
Removes a previously configured PLMN identifier for the GGSN service.

mcc mcc_number
Specifies the mobile country code (MCC) portion of the PLMN’s identifier. 
mcc_number is the PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc mnc_number
Specifies the mobile network code (MNC) portion of the PLMN’s identifier. 
mnc_number is the PLMN MNC identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.

primary
When multiple PLMN IDs are configured the primary keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute (3GPP-GGSN-MCC-MNC).

Usage
The PLMN identifier is used to aid the GGSN service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple GGSN services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each GGSN Service.

Example
The following command configures the PLMN identifier with an MCC of 462 and MNC of 2:

plmn id mcc 462 mnc 02
plmn unlisted-sgsn

Configures the GGSN’s policy for handling communications from SGSNs that it is not configured to communicate with.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax


**default**

 Resets configured parameters to their default settings.

**foreign**

 Default: Disabled
 Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the sgsn command.
 This keyword also dictates that unlisted SGSNs are treated as if they belong to a foreign PLMN. Therefore PDP contexts originating from them are treated as visiting or roaming.

**disable-gtpc-echo**

 Default: Send GTPC Echo messages to unlisted SGSNs.
 When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

**reject-foreign-subscriber**

 Default: Disabled
 Specifies that incoming calls from foreign subscribers are rejected.

**home**

 Default: Disabled
 Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the sgsn command.
 This keyword also dictates that unlisted SGSNs are treated as if they belong to the GGSN service’s home PLMN.

**reject**

 Default: Enabled
 Specifies that the GGSN service rejects messages from SGSNs that are not configured within the service using the sgsn command.
 When the GGSN service rejects the message(s), it returns a cause code of No Resources 199 (C7H, No resources available).
GGSN Service Configuration Mode Commands

Usage
This command works in conjunction with the sgsn command that configures the GGSN service to communicate with specific SGSNs. Any messages received from SGSNs not configured in that list are subject to the rules dictated by the unlisted-sgsn policy.

Example
The following command configures the GGSN service to accept messages from unlisted SGSNs and treat the SGSN as if it is on the GGSN’s home network:

```
plmn unlisted-sgsn accept home
```
**policy**

Specifies the reject code to be used in the "Create PDP Context" response message when a RADIUS server timeouts.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
policy {accounting-server-timeout use-reject-code {system-failure | no-resources } | authentication-server-timeout use-reject-code {system-failure | user-authentication-failure } }

default policy {authentication-server-timeout | accounting-server-timeout }
```

**default**

Restores the specified parameter to its default setting.

```
accounting-server-timeout use-reject-code {system-failure | no-resources }
```

Default: **no-resources**

Specifies the reject code used by the GGSN if communication with an accounting server times out. The possible reject codes are:

- system-failure (204 (CCH))
- no-resources (199 (C7H))

```
authentication-server-timeout use-reject-code {system-failure | user-authentication-failure }
```

Default: user-authentication-failure

Specifies the reject code used by the GGSN if communication with an authentication server times out. The possible reject codes are:

- system-failure (204 (CCH))
- user-authentication-failure (209 (D1H))

**Usage**

This command is used to configure the cause code used by the GGSN if communication with either a RADIUS authentication or accounting server times out. When this parameter is used in conjunction with Radius accounting servers, the response is only set if a flag is configured in the APN Delay GTP Response, only after getting a response to the Accounting Start.

**Example**

The following command configures the GGSN response to a RADIUS authentication server timeout to be system-failure:
policy authentication-server-timeout use-reject-code system-failure
retransmission-timeout

Configures the timeout period in between retransmissions of GTP control packets. This timeout configuration is not applicable on Echo Request retransmission.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax
retransmission-timeout retransmit_time

retransmit_time
Default: 5
Specifies the amount of time that must pass without an SGSN response before the GGSN service retransmits GTP control packets. 
retransmit_time is measured in seconds and can be configured to any integer value between 1 and 20.

Usage
This command is used in conjunction with the `max-retransmissions` command to control the retransmission of GTP control packets when no response is received from an SGSN.
If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of the max-retransmissions command.
If the max-retransmissions value is exceeded within the retransmission-timeout period, the GGSN records a “Path Failure” for that SGSN and releases all PDP contexts associated with it.

Important: This retransmission timeout configuration is not applicable for Echo Requests message retransmission. Echo are sent/retransmitted every echo interval, which can be configured separately.

Example
The following command configures a timeout value of 20 seconds:

```
retransmission-timeout 20
```
**setup-timeout**

Configures the maximum amount of time the GGSN service allows for the setting up of PDP contexts.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
setup-timeout setup_time
```

- `setup_time`
  - Default: 60
  - Specifies the maximum amount of time the GGSN service allows for the setting up of PDP contexts.
  - `setup_time` is measured in seconds and can be configured to any integer value between 1 and 6000.

**Usage**

Use this command to limit the amount of time allowed for setting up PDP contexts. If the PDP context is not set up within the configured time frame, the GGSN service rejects the PDP context with a cause code of 199 (C7H, No resources available).

**Example**

The following command allows a maximum of 120 seconds for the setting up of PDP contexts:

```
setup-timeout 120
```
**sgsn address**

Configures the SGSNs that this GGSN service is allowed to communicate with.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
sgsn address {{ip_address [subnetmask netmask ]} | ip_address/netmask} [plmn-
foreign [reject-foreign-subscriber] | mcc mcc_code mnc mnc_code [reject-foreign-
subscriber]] [rat-type {GAN | GERAN | HSPA | UTRAN | WLAN }] [description

description] [disable-gtpc-echo]

no sgn (address ip_address [subnetmask netmask ] )
```

---

**no**
Removes a specific SGSN from the list or all configured SGSNs.

**address**
Configures the IP address of the SGSN.
`ip_address` must be expressed in dotted decimal notation.

**subnetmask**
Configures the subnet mask of the SGSN.
`netmask` must be expressed in dotted decimal notation.

**disable-gtpc-echo**
Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

**plmn-foreign**
Indicates whether or not the SGSN belongs to a foreign public land mobile network (PLMN).

**reject-foreign-subscriber**
Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

**mcc mcc_code**
Specifies the mobile country code (MCC) portion of the PLMN’s identifier.
`mcc_code` is the PLMN MCC identifier and can be configured to any integer value between 100 and 999.

**mnc mnc_code**
Specifies the mobile network code (MNC) portion of the PLMN’s identifier.
mnc_code is the PLMN MNC identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.

rat-type {GAN | GERAN | HSPA | UTRAN | WLAN }

This keyword configures the type of radio access technology.
GAN: Specifies the Generic Access Network type of RAT.
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

description description

Add description field to the SGSN entry in GGSN service.
description is a string of 1 to 63 alpha and/or numeric characters.

Usage

Use this command to configure a list of SGSNs that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSNs.

Important: The GGSN only communicates with the SGSNs configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the plmn unlisted-sgsn command.

Example

The following command configures the GGSN to communicate with an SGSN on a foreign PLMN with an IP address of 192.168.1.100 and subnet mask of 255.255.255.0:

sgn address 192.168.1.100 subnetmask 255.255.255.0 plmn-foreign
sgsn define-multiple-address-group

This keyword defines an SGSN Multiple Address Group and enters SGSN Multiple Address Group Configuration mode. Whenever there is a change in the control address in a GTPC UPC message, it is treated as an inter-SGSN handoff because an SGSN is usually identified uniquely by a single IP-address. This command supports a multiple address group feature which allows you to specify a set of addresses that specify a single SGSN. When a UPC handoff is received from any address in the group, it is treated as an intra-SGSN handoff.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

[no] sgsn define-multiple-address-group grp_name

-no
Removes a specific SGSN Multiple Address Group from the list GGSN service configuration.

-grp_name
Specifies the name of an SGSN multiple address group to create or configure. must be an alphanumeric string from 1 through 63 characters in length.

Usage
Use this command to create or configure an SGSN Multiple Address Group that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSN Multiple Address Groups.

Example
The following command creates an SGSN Multiple Address Group named sgsngrp1 enters SGSN Multiple Address Group Configuration mode:

sgsn define-multiple-address-group sgsngrp1
sgsn multiple-address-group

Configures the SGSN multiple address groups that this GGSN service is allowed to communicate with.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

sgsn multiple-address-group grp_name [disable-gtpc-echo] [mcc mcc_code mnc mnc_code [reject-foreign-subscriber]] [plmn-foreign [reject-foreign-subscriber] [rat-type {GAN | GERAN | HSPA | UTRAN | WLAN }]] [description description ]

no sgsn multiple-address-group grp_name

no
Removes a specific SGSN multiple address group from the list of configured SGSN multiple address groups.

 grp_name
Specifies the name of a configured SGSN multiple address group to use.

disable-gtpc-echo
Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

plmn-foreign
Indicates whether or not the SGSN multiple address group belongs to a foreign public land mobile network (PLMN).

reject-foreign-subscriber
Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

mcc mcc_code
Specifies the mobile country code (MCC) portion of the PLMN’s identifier.
mcc_code is the PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc mnc_code
Specifies the mobile network code (MNC) portion of the PLMN’s identifier.
mnc_code is the PLMN MNC identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.

rat-type {GAN | GERAN | HSPA | UTRAN | WLAN }
This keyword configures the type of radio access technology.
**GGSN Service Configuration Mode Commands**

**sgsn multiple-address-group**

**GAN:** Specifies the Generic Access Network type of RAT.

**GERAN:** Specifies the GSM EDGE Radio Access Network type of RAT.

**HSPA:** Specifies the High Speed Packet Access type of RAT.

**UTRAN:** Specifies the UMTS Terrestrial Radio Access Network type of RAT.

**WLAN:** Specifies the Wireless Local Access Network type of RAT.

**description description**

Add a description field to the SGSN multiple address group entry in the GGSN service configuration. *description* must be a string of 1 through 63 alphanumeric characters.

**Usage**

Use this command to configure a list of SGSN multiple address groups that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSN multiple address groups.

**Important:** The GGSN only communicates with the SGSN multiple address groups configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the `plmn unlisted-sgsn` command.

**Example**

The following command configures the GGSN to communicate with an SGSN with multiple address that is defined by an SGSN multiple address group named `sgsngrp1` that is on a foreign PLMN:

```plaintext
sgsn multiple-address-group sgsngrp1 plmn-foreign
```
Chapter 103
Global Configuration Mode Commands

The Global Configuration Mode is used to set basic system wide options.

Exec Mode
  configure
  Global Configuration Mode
aaa accounting-overload-protection

This command configures Overload Protection Policy for accounting requests.

Product
All

Privilege
Security Administrator, Administrator

Syntax

aaa accounting-overload-protection prioritize-gtpp

{ default | no } aaa accounting-overload-protection

---

default
Configures the default setting.
Default: no priority assigned

---

no
Disables the Overload Protection configuration.

---

prioritize-gtpp
Specifies to give higher priority to GTPP requests among the other outstanding requests. So while purging the lower priority requests will be selected first.

Usage
Use this command to configure Overload Protection Policy for accounting requests.

Example
The following command prioritizes GTPP requests among the other outstanding requests:

    aaa accounting-overload-protection prioritize-gtpp
aaa default-domain

Configure global accounting and authentication default domain for subscriber and context-level administrative user sessions.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
aaa default-domain { administrator | subscriber } domain_name
no aaa default-domain { administrator | subscriber } [ domain_name ]
```

**no**
Removes all or only the specified configured domain.

**administrator | subscriber**

- **administrator**: Configures the default domain for context-level administrative users.
- **subscriber**: Configures the default domain for subscribers.

**domain_name**
Specifies the context which is to be set as the default. *domain_name* must be from 1 to 79 alpha and/or numeric characters with no spaces.

Usage

This command configures the default domain which is used when accounting and authentication services are required for context-level administrative user and subscriber sessions whose user name does not include a domain.

Example

The following commands configure the default domains for context-level administrative users and subscribers, respectively:

```
aaa default-domain administrator sampleAdministratorDomain
aaa default-domain subscriber sampleSubscriberDomain
```

The following command removes the sampleSubscriberDomain domain:

```
no aaa default-domain subscriber sampleSubscriberDomain
```
aaa domain-matching ignore-case

This command disables case sensitivity when performing domain matching. When this command is enabled, the system disregard case when matching domains.

Product
All

Privilege
Security Administrator, Administrator

Syntax
[ no ] aaa domain-matching ignore-case

default aaa domain-matching

default
Configures ignore-case as the domain matching method.

no
Specifies that the system consider case when domain matching.

Usage
Use this command to configure the system to ignore case when matching domains.

Example
The following command configures the system to ignore case when matching domains:

aaa domain-matching ignore-case
aaa domain-matching imsi-prefix

This command enables domain lookup for session based on the IMSI prefix length. Default: Disabled

**Important:** This command is only available in Release 8.3 and later.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
aaa domain-matching imsi-prefix prefix-length prefix_length

no aaa domain-matching imsi-prefix
```

**Usage**

Use this command to configure the IMSI-prefix method of domain matching. This command enables domain lookup for the session based on the IMSI prefix length. If there is a domain configured with the matching IMSI prefix, the associated configuration is used. This feature does not support partial matches.

**Example**
The following command configures the IMSI prefix method for domain matching setting the prefix length to 10.

```plaintext
aaa domain-matching imsi-prefix prefix-length 10
```
aaa large-configuration

This command enables/disables the system to accept a large number of RADIUS configurations to be defined and
stored.

**Important:** For this command to take affect, after entering the command the configuration must be saved and
reloaded.

When aaa large-configuration is disabled, the following restrictions are in place:

- Only one (1) NAS IP address can be defined per context with the `radius attribute` command.
- The RADIUS attribute `nas-ip-address` can only be configured if the RADIUS group is `default`.
- Only 320 RADIUS servers can be configured system-wide.
- Only 64 RADIUS groups can be configured system-wide.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
aaa large-configuration
no aaa large-configuration
```

**Usage**

When aaa large-configuration is enabled, the system provides the ability to configure multiple NAS IP
addresses in a single context to used with different radius groups. As well, the command allows support for
up to 1600 RADIUS server configurations and for a PDSN a maximum of 400 or for a GGSN a maximum of
800 RADIUS server group configurations system-wide.

**Example**

To enable the definition of a large number of RADIUS configurations, enter the following commands in the following
order:

In APN Configuration mode, use the `aaa group` command and enter:

```
default aaa group
```

In Global Configuration mode, enter

```
aaa large-configuration
```
In Exec mode, use the `save configuration` command and then the `reload` command.
aaa last-resort

Configure global accounting and authentication last resort domain for subscriber and context-level administrative user sessions.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
aaa last-resort context { administrator | subscriber } context_name
no aaa last-resort context { administrator | subscriber } [ context_name ]
no
Removes all or only the specified previously configured authentication last resort domain name.

administrator | subscriber
administrator: Configures the last resort domain for context-level administrative.
subscriber: Configures the last resort domain for the subscribers.

context_name
Specifies the context which is to be set as the last resort. context_name must be from 1 to 79 alpha and/or numeric characters with no spaces.

Usage
Set the last resort context which is used when there is no applicable default domain (context) and there is no domain provided with the subscriber’s or context-level administrative user’s name for use in the AAA functions.

Example
The following commands configure the last resort domains for context-level administrative user and subscribers, respectively:

aaa last-resort administrator sampleAdministratorDomain
aaa last-resort subscriber sampleSubscriberDomain

The following command removes the previously configured domain called sampleAdministratorDomain:

no aaa last-resort administrator sampleAdministratorDomain```
aaa username-format

Configure global accounting and authentication user name formats for AAA functions. Up to six formats may be configured.

Product
All

Privilege
Security Administrator, Administrator

Syntax

aaa username-format { domain | username } separator

no aaa username-format { domain | username } separator

no
Removing the specified user name format from the configuration.

domain | username
Default: username @
domain: indicates the left side of the string from the separator character is a domain name and the right side is the user name.
username: indicates the left side of the string from the separator character is a user name and the right side is the domain name.

Important: The user name string is always searched from right to left for the first occurrence of the separator character.

separator
Specifies the character to use for delimiting the domain from the user name for global AAA functions as one of: @, %, -, \, #, or /. Note: to specify a slash (\) as the separator it is necessary to enter a double slash (\\) on the command line.

Usage
Define the formats for user name delimiting if certain domains or groups of users are to be authenticated based upon their user name versus domain name.

Example

aaa username-format domain @

aaa username-format username @

no aaa username-format username @
aaa username-format
active-charging service

This command creates/selects an Active Charging Service.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
active-charging service ecs_service_name [ -noconfirm ]

no active-charging service ecs_service_name
```

**no**
Removes the specified Active Charging Service.

**ecs_service_name**
Creates/selects the specified Active Charging Service, and changes to the Active Charging Service Configuration Mode.

*ecs_service_name* must be an alpha and/or numeric string of 1 through 15 characters in length.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**
Use this command to create/select an active charging service on the system.

Use this command after enabling Enhanced Charging Service using the `require active-charging` command. This command allows administrative users to configure the Enhanced Charging Service functionality.

**Example**
The following command creates an active charging service named *test*:

```
active-charging service test
```
alarm

Enables/disables alarming options for the switch processor card internal alarms and the central-office external alarms. To verify the state of the alarms, refer to the `show alarm` command.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
alarm { audible | central-office }
no alarm { audible | central-office }
```

**Usage**
Disables the option specified.

- `audible`: indicates the internal audible alarm on the switch processor cards are to be enabled.
- `central-office`: indicates the central office alarms are to be enabled.

**Example**
The following commands enable the SMC internal alarm and disable the central office alarms, respectively.

```plaintext
alarm audible
no alarm central-office
```
arp

Configures a system-wide time interval for performing Address Resolution Protocol (ARP) refresh.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
arp base-reachable-time time

default arp base-reachable-time
```

```
default
Restores the parameter to its default setting.

time
Default: 30
Specifies the ARP refresh interval (in seconds). The range is 30 to 86400 seconds.
```

Usage
Use this command to configure a system-wide ARP refresh interval. Once a neighbor is found, the entry is considered valid for at least a random value between the time/2 and the time*1.5.

Example
The following command configures an ARP refresh interval of 1 hour:

```
arp base-reachable-time 3600
```
autoconfirm

This command disables or enables confirmation for certain commands. This command affects all future CLI sessions.

---

**Important:** To change the behavior for the current CLI session only, use the `autoconfirm` command in the Exec Mode.

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator, Operator</td>
</tr>
</tbody>
</table>

**Syntax**

```
autoconfirm

no autoconfirm
```

**Usage**

When autoconfirm is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When autoconfirm is disabled the confirmation questions never appear. Disabling autoconfirm disables command confirmation for all future CLI sessions. By default `autoconfirm` is enabled.

**Example**

The following command enables command confirmation for all future CLI sessions;

```
autoconfirm
```

The following command disables command confirmation for all future CLI sessions;

```
no autoconfirm
```
autoless

This command is obsolete. It is included in the CLI for backward compatibility with older configuration files. When executed, this command issues a warning and performs no function.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
autoless

no autoless
```
banner

Configures the CLI banner which is displayed upon the initialization of a CLI session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
banner { charging-service | lawful-intercept | motd | pre-login } string
no banner { charging-service | lawful-intercept | motd | pre-login }
```

**no**
Removes the banner message by setting it to be string of zero length.

### charging-service

Specifies the Enhanced Charging Service banner message. That banner is displayed upon the initialization of an SSH CLI session with ECS-admin privileges (whenever anyone with the CLI privilege bit for ECS logs in).

### lawful-intercept

Configures the CLI banner message of the day which is displayed upon the initialization of an SSH CLI session with li-admin privileges.

### motd

Configures the CLI banner message of the day which is displayed upon the initialization of any CLI session.

### pre-login

Configures the CLI banner displayed before a CLI user logs in.

**Important:** This banner is displayed only for serial port and telnet log ins. It is not supported in ssh and, therefore, will not be displayed before ssh log ins.

### string

Specifies the banner or message to be displayed at session initialization. `string` may be from 0 to 2048 characters and must be enclosed in double quotation marks if the banner or message is to include spaces.

**Usage**

Set the message of the day banner when an important system wide message is needed. For example, in preparation for removing a chassis from service, set the banner 1 or more days in advance to notify administrative users of the pending maintenance.
Example

banner motd "Have a nice day."

banner motd No_News_Today

no banner motd
**boot**

The commands in this section set system boot time parameters.
boot delay

Configures the delay period, in seconds, before attempting to boot the system from a software image file residing on an external network server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
boot delay time

no boot delay
```

- **no**
  Deletes the setting for the boot delay. The boot process executes immediately.

- **time**
  Specifies the amount of time (in seconds) to delay prior to requesting the software image from the external network server. The range is 1 to 300 seconds.

Usage
Useful when booting from the network when connection delays may cause timeouts. Such as when the Spanning Tree Protocol is used on network equipment.

**Important:** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

Example
The following sets the boot delay to 10 seconds:

```
boot delay 10
```
boot interface

Configures the Switch Processor I/O card network interfaces for obtaining a system software image during the system boot process.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
boot interface { spio-eth1 | spio-eth2 } [ medium { auto | speed medium_speed duplex medium_duplex } [ media medium_media ] ]
```

```
o boot interface
```

no

Removes the boot interface configuration from the boot.sys file. Only files from the local file system can be loaded.

```
spio-eth1 | spio-eth2
```

Specifies the network interface to be configured where spio-eth1 is the primary interface on the SPIO (slot 24 interface 1 or slot 25 interface 1) and spio-eth2 is the secondary interface on the SPIO (slot 24 interface 2 or slot 25 interface 2). The interfaces refer to either the RJ-45 interfaces for speeds of 10, 100, or 1000 megabit per second (Mbps) or the SFP interface for the optical gigabit (1000 Mbps) interface.

```
medium { auto | speed medium_speed duplex medium_duplex }
```

Default: auto

**auto:** configures the interface to auto-negotiate the interface speed and duplex.

**speed medium_speed duplex medium_duplex:** specifies the speed to use at all times where medium_speed must be one of:

- 10
- 100
- 1000

The keyword **duplex** is used to set the communication mode of the interface where medium_duplex must be one of:

- full
- half

```
media medium_media
```

Default: rj45

Optionally sets the physical interface where medium_media must be either rj45 or sfp.
Modify the boot interface settings to ensure the system is able to obtain a software image from an external network server.

**Important:** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**
The following configures the primary interface to auto-negotiate the speed.

```plaintext
boot interface spio-eth1 medium auto
```

The following command configures the secondary interface to a fixed gigabit speed at full duplex using RJ45 connectors for the physical interface.

```plaintext
boot interface spio-eth2 medium speed 1000 duplex full media rj45
```

The following restores the defaults for the boot interface.

```plaintext
no boot interface
```
**boot nameserver**

Configures the IP address of the DNS (Domain Name Service) server to use when looking up hostnames in URLs for network booting.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
boot nameserver ip_address
no boot nameserver
```

**ip_address**
IPv4 address of the DNS server the system uses to lookup hostnames in URLs for a software image from the network during the system boot process.

**no**
Removes the network boot nameserver information from the boot.sys file.

**Usage**
Use this command to identify the DNS server to use to lookup hostnames in a software image URL.

**Important:** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**
The following configures the system to communicate with a DNS nameserver with the IP address of 1.2.3.4:

```
boot nameserver 1.2.3.4
```


## boot networkconfig

Configures the networking parameters for the Switch Processor I/O card network interfaces to use when obtaining a software image from an external network server during the system boot process.

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax

```plaintext
bootnetworkconfig { dhcp | { dhcp-static-fallback | static } ipaddress spio24 ip_address [ spio25 ip_address ] netmask ip_mask [ gateway gw_address ] } }

no boot networkconfig
```

- **no**
  
  Removes the network configuration information from the boot.sys file.

- **dhcp**

  Indicates that a Dynamic Host Control Protocol (DHCP) server is used for communicating with the external network server.

- **dhcp-static-fallback | static**

  - **dhcp-static-fallback**: provides static IP address fallback network option when a DHCP server is unavailable.
  - **static**: specifies a fixed network IP address for the external network server that hosts the software image.

- **spio24 ip_address [ spio25 ip_address ] netmask ip_mask [ gateway gw_address ]**

  - **spio24 ip_address [ spio25 ip_address ]**: the IP address to use for the SPIO in slot 24 and optionally the SPIO in slot 25 for network booting. `ip_address` must be specified using the standard IPv4 dotted-decimal notation.
  - **netmask ip_mask**: the network mask to use in conjunction with the IP address(es) specified for network booting. `ip_mask` must be specified using the standard IPv4 dotted-decimal notation.
  - **gateway gw_address**: the IP address of a network gateway to use in conjunction with the IP address(es) specified for network booting. `gw_address` must be specified using the standard IPv4 dotted-decimal notation.

- **Important:** If `gw_address` is not specified, then the network server must be on the same LAN as the system. Since both SPIOS must be in the same network, the netmask and gateway settings are shared.

### Usage
Configure the network parameters for the ports on the SPIO cards to use to communicate with an external network server that hosts software images.

**Important:** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Important:** When configuring static addresses both SPIOs must have different IP addresses. Neither address can be the same as the local context IP address.

**Example**
The following configures the system to communicate with the external network server via DHCP with a fallback to IP address 1.2.3.4, respectively.

```
boot networkconfig dhcp-static-fallback ip address spio24 192.168.100.10 netmask 255.255.255.0
```

The following command configures the system to communicate with an external network server using the fixed (static) IP address 1.2.3.4 with a network mask of 255.255.255.0.

```
boot networkconfig static ip address spio24 192.168.100.10 netmask 255.255.255.0
```

The following restores the system default for the network boot configuration options.

```
no boot networkconfig
```
**boot system priority**

Specifies the priority of a boot stack entry to use when the system first initializes or restarts. Up to 10 boot system priorities (entries in the boot.sys file located on the /flash device in the SMC) can be configured.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
boot system priority number image_image_url config config_path
no boot system priority number
```

- `no` Remove a boot stack entry at the priority specified from the boot stack when it is no longer used.

- `priority number`
  Specifies the priority for the file group (consisting of an image (.bin) and its corresponding configuration (.cfg) file) specified in the boot stack. The value must be in the range from 1 through 100 where a priority of 1 is the highest. Up to 10 boot system priorities (boot stack entries) can be configured.

**Important**: When performing a software upgrade it is important that the new file group have the highest priority (lowest value) configured.

**Important**: It is suggested that an “N-1” priority numbering methodology, where “N” is the first priority in the current boot stack be employed to ensure that higher priority numbers remain open.

- `image image_url`
  Specifies the location of a image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted according to one of the following formats:
  - ASR 5000:
    - `[file:][/flash[/pcmcia[/hd]][/directory]/filename`
  - `[http:|tftp://host[:port][/directory]/filename`

**Important**: Use of the SMC hard drive is not supported in this release.

- `directory` is the directory name.
- `filename` is the actual file of interest.
- `host` is the IP address or host name of the server.
- `port#` is the logical port number that the communication protocol is to use.
**Important:** A file intended for use on an ASR 5000 uses the convention xxxxx.asr5000.bin, where xxxxx is the software build information.

**Important:** When using the TFTP, it is advisable to use a server that supports large blocks, per RFC 2348. This can be implemented by using the “block size option” to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

```
config config_path
```

Specifies the location of a configuration file to use for system startup. This must be formatted according to the following format:

- ASR 5000:
  ```
  [{file:}|/flash|/pcmcia1|/pcmcia2]{/path}/filename
  ```

- Important: Use of the SMC hard drive is not supported in this release.

Where `path` is the directory structure to the file of interest, and `filename` is the name of the configuration file. This file typically has a `.cfg` extension.

**Usage**

This command is useful in prioritizing boot stack entries in the boot.sys file, typically located on the /flash device of the Active SMC, for automatic recovery in case of a failure of a primary boot file group.

**Important:** The configuration file must reside on the SMC’s local filesystem, stored on one of its local devices (/flash, /pcmcia1, /pcmcia2, /hd). Attempts to load the configuration file from an external network server will result in a failure to load that image and configuration file group, causing the system to load the image and configuration file group with the next highest priority in the boot stack.

**Important:** Configuration changes do not take effect until the system is reloaded.

**Important:** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**

The following commands set up two locations to obtain a boot file group from.

```
boot system priority 1 image tftp://remoteABC/pub/2003jan.bin config
/flasb/pub/data/2003feb.cfg
```

```
boot system priority 2 image /flash/pub/data/2002jun.bin config
/pcmcia1/pub/data/2003feb.cfg
```

The following removes the current priority 1 boot entry from the boot.sys file.
no boot system priority 1
bulkstats

Enables the collection of bulk statistics by the system and/or enters the bulk statistic configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

bulkstats { collection | historical | mode }

no bulkstatscollection

no
Disables the collection of bulk statistics.

collection
Enables the statistics collection process. Collects a period snapshot of data, i.e. “here is what the value is right now”.

historical collection
Enables the system to collect historical bulk statistics. If enabled, the system keeps track of some things which require the storing of more data, such as “the highest value that’s been seen over the last 24 hours”.

mode
Enters the bulk statistics configuration mode. The resulting command-line prompt will look similar to:

[<context-name>]asr5000(config-bulkstats)#

Usage

The Bulk Statistics Configuration Code consists of commands for configuring bulk statistic properties, such as the period of collection. Bulk Statistics configuration mode commands are defined in the “Bulk Statistics Configuration Mode Commands” chapter.
The system can be configured to collect bulk statistics and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group or schema, for example, system stats, port stats, radius stats.
Once bulk statistics receiver, schema, and collection properties are configured, this bulkstats command is used to enable or disable the collection of the data.
To collect a sample that will provide an average, for example, an average of CPU counters, the “historical” features must be enabled with the bulkstats historical collection command.
Since bulk statistics are collected at regular, user-defined intervals, the bulkstats force command in the Exec Mode can be used to manually initiate the collection of statistics at any time.
Example

bulkstats collection
bulkstats mode
no bulkstats collection
ca-certificate

Configures and selects an X.509 CA root certificate to enable a security gateway to perform certificate-based peer (client) authentication. The system supports a maximum of 16 certificates and 16 CA root certificates. A maximum of four CA root certificates can be bound to a crypto template.

Product Privilege

Administrator, Security Administrator, Operator

Syntax

[ no ] ca-certificate name name pem { data pemdata | url url }

no
Removes the named CA certificate.

name
Names the CA certificate.

pem data pemdata | url
The PEM-formatted data can be specified (data pemdata) or the information can be read from a file via url url). When read via a file, note that show configuration will not contain the url reference, but will instead output the data via data pemdata such that the configuration file is self-contained.

Usage

In addition to the X.509 certificate-based gateway authentication method and the PSK (Pre-Shared Key) and EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) peer (client) authentication methods, the FNG supports X.509 certificate-based peer authentication.

The FNG checks the network policy on whether a FAP is authorized to provide service. If the network policy states that all FAPs that pass device authentication are authorized to provide service, no further authorization check may be required. If the network policy requires that each FAP be individually authorized for service (in the case where the FEID is associated with a valid subscription), the FNG sends a RADIUS Access-Request message to the AAA server. If the AAA server sends a RADIUS Access-Accept message, the FNG proceeds with device authentication. Otherwise, the FNG terminates the IPSec tunnel setup by sending an IKEv2 Notification message indicating authentication failure.

The operator/administrator is responsible for configuring the certificates through the CLI. The FNG will generate an SNMP notification when the certificate is within 30 days of expiration, and then once a day.

Example

Use the following command to remove a certificate named fap1:

no ca-certificate data fap1
card

Enters the card configuration mode for the card specified.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
card number
```

`number`
Specifies the number of the card for which the card configuration mode is to be entered. `number` must be a value in the range 1 through 48.

Usage
Enter the configuration mode for a specific card when changes are required.

**Important:** This command is not supported on all platforms.

Example

```
card 8
```
card-standby-priority

Configures the redundancy priorities for the Packet Services Cards (PSC or PSC2) by specifying the slot number search order for a standby card when needed. Not available for the XT2 platform.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
    card-standby-priority slot_num [ slot_num ] [ slot_num ] ...
```

*slot_num*
Specifies the slot of the card for the order of the standby cards. *slot_num* must be in the range from 1 through 16 excluding slots 8 and 9. *slot_num* may be repeated as many times as necessary to indicate the complete search order.

**Usage**
Set the standby order of the redundant cards when multiple standby cards are available. Questionable hardware should be placed lower in the priority list.

**Important:** This command replaces the `psc-standby-priority` command.

**Important:** This command is not supported on all platforms.

**Example**
The following command configures the redundancy priority to use the standby cards in slots 16, 14, and 12 in that order:

```
    card-standby-priority 16 14 12
```
**cdr-multi-mode**

This command enables multiple instances of CDRMOD.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default ] cdr-multi-mode
```

- `default`
  Configures the default setting.

**Usage**

Use this command to enable multiple instances of CDRMOD.
certificate

Configures and selects an X.509 Trusted Author certificate.

Product

ECS
PDG/TTG
PDIF

Privilege

Administrator, Security Administrator, Operator

Syntax

[ no ] certificate name name pem { data pemdata | url url }

no
Removes the named certificate.

name
Names the certificate.

data pemdata | url
The PEM-formatted data can be specified (data pemdata) or the information can be read from a file via url. When read via a file, note that show configuration will not contain the URL reference, but will instead output the data via data pemdata, such that the configuration file is self-contained.

Usage

A certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.
If CERT information is configured, PDIF will include the CERT payload in the first IKE_AUTH Response during the first authentication. PDIF stores its own certificate for use in the first AUTH calculation. MS will not have its own certificate from CA. Still it will be capable of accepting a certificate from PDIF and verify AUTH.
The operator/administrator is responsible for configuring the certificates through the CLI. PDIF will generate an SNMP notification when the certificate is within 30 days of expiration, and then once a day.

Example

Use the following command to remove a certificate named box1:

no certificate data box1
cli

Configures global CLI parameters.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
cli { access { monitor-protocol | monitor-subscriber } { administrator | operator } | login-failure-delay number | max-sessions number | operator clear-subscriber-one-only | trap config-mode }

no cli { max-sessions | login-failure-delay number | operator clear-subscriber-one-only | trap config-mode }

default cli { access { monitor-protocol | monitor-subscriber } | max-sessions | login-failure-delay number | operator clear-subscriber-one-only | trap config-mode }
```

no

Removes the limit on the number of allowed simultaneous CLI sessions on the system, or removes the limit of how many subscribers an Operator can clear.

default

Resets the keywords to their default values.

access { monitor-protocol | monitor-subscriber } { operator | administrator }

Sets access privileges on the `monitor-template` and `monitor-queue` commands: `monitor-protocol`: Selects privileges for the `monitor-template` command. `monitor-subscriber`: Selects privileges for the `monitor-template` command. `operator`: Sets the privileges for the selected command to allow use by users with operator privileges. `administrator`: Restricts use of the selected command to administrators only.

login-failure-delay number

This is the time to wait before a login failure is returned and another login may be attempted. Default is five seconds.

max-sessions number

Sets the number of allowed simultaneous CLI sessions on the system. If this value is set to a number below the current number of open CLI sessions, the open sessions will continue until closed. `number` must be from 2 through 100.
Caution: Use caution when setting this command. Limiting simultaneous CLI sessions prevents authorized users from accessing the system if the maximum number allowed has been reached. The system already limits CLI sessions based on available resources. Additional limitation could have adverse effects.

**operator clear-subscriber-one-only**
Restricts Operator to clearing only one subscriber session at a time.

**trap config-mode**
Enables sending an SNMP notification (trap) when a CLI user enters the configuration mode.

Usage
Control the number of simultaneous CLI sessions on the system at any given time.

**Important:** The maximum number of multiple CLI session support is based on the amount of available memory. The Resource Manager, however, reserves enough resources so that a minimum of 15 CLI sessions are assured for ASR 5000s. One of the CLI sessions is reserved for use exclusively by a CLI session on an SPIO console interface. Additional CLI sessions beyond the pre-reserved set are permitted if sufficient SMC resources are available. If the Resource Manager is unable to reserve resources for a CLI session beyond those that are pre-reserved, administrative users are prompted as to whether or not the system should attempt to create the new CLI session even without reserved resources.

Example
The following command sets the number of allowed simultaneous CLI sessions to 5.

`cli max-sessions 5`

The following command sets the command `monitor protocol` to administrator-only

`cli access monitor-protocol administrator`
clock

Configures system clock timezone and what local time zone to use.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
clock timezone tz [ local ]
no clock timezone
```

**no**
Resets the system timezone to the system default UTC.

**tz**
Specifies the system time zone to use as one of:

- `america-buenos-aires` (GMT-3:00; Buenos Aires)
- `america-caracas` (GMT-4:00; Caracas)
- `america-guatemala` (GMT-6:00; Guatemala, Guatemala)
- `america-la_paz` (GMT-4:00; La Paz)
- `america-lima` (GMT-5:00; Lima, Peru)
- `america-puerto-rico` (GMT-4:00; Puerto Rico)
- `america-sao-paulo` (GMT-3:00; Brazil)
- `america-tijuana` (GMT-8:00; Tijuana)
- `asia-baghdad` (GMT+3:00; Baghdad, Russia Zone 2, Kuwait, Nairobi, Riyadh, Moscow, Tehran)
- `asia-bangkok` (GMT+7:00; Bangkok)
- `asia-calcutta` (GMT+5:30; Calcutta, Mumbai, New Delhi)
- `asia-dhaka` (GMT+6:00; Dhaka)
- `asia-hong-kong` (GMT+8:00; Hong_Kong)
- `asia-irkutsk` (GMT+9:30; Irkutsk)
- `asia-kabul` (GMT+4:30; Kabul)
- `asia-karachi` (GMT+5:00; Karachi)
- `asia-kathmandu` (GMT+5:45; Kathmandu)
- `asia-magadan` (GMT+11:00; Magadan)
- `asia-muscat` (GMT+4:00; Abu Dhabi, UAE, Muscat, Tblisi, Volgograd, Kabul)
- `asia-rangoon` (GMT+6:30; Rangoon)
- `asia-seoul` (GMT+9:00; Seoul)
- asia-tehran (GMT+3:30; Tehran)
- asia-tokyo (GMT+9:00; Tokyo, Russia Zone 8)
- atlantic-azores (GMT-2:00; Azores)
- atlantic-cape-verde (GMT-1:00; Cape Verde Islands)
- australia-perth (GMT+8:00) Perth
- australia-darwin (GMT+9:30) Northern Territory - Alice Springs, Darwin, Uluru
- australia-adelaide (GMT+9:30) Southern Territory - Adelaide
- australia-melbourne (GMT+10:00) Victoria - Ballarat, Melbourne
- australia-sydney (GMT+10:00) New South Wales - Newcastle, Sydney, Wollongong
- australia-hobart (GMT+10:00) Tasmania - Hobart, Launceston
- australia-brisbane (GMT+10:00) Queensland - Brisbane, Cairns, Toowoomba, Townsville
- australia-lordhowe (GMT+10:30) Lord Howe Island
- canada-newfoundland (GMT-3:30; Newfoundland)
- canada-saskatchewan (GMT-6:00; Saskatchewan)
- europe-central (GMT+1:00; Paris, Berlin, Amsterdam, Brussels, Vienna, Madrid, Rome, Bern, Stockholm, Oslo)
- europe-dublin (GMT+0:00) Dublin, Ireland
- europe-eastern (GMT+2:00; Russia Zone 1, Athens, Helsinki, Istanbul, Jerusalem, Harare)
- newzealand-auckland (GMT +12:00; Auckland, Wellington)
- newzealand-chatham (GMT +12:45; Chatham)
- nuku (GMT-13:00; Nuku'alofa)
- pacific-fiji (GMT+12:00; Wellington, Fiji, Marshall Islands)
- pacific-guam (GMT+10:00; Brisbane, Cairns, Sydney, Guam)
- pacific-kwajalein (GMT-12:00; Kwajalein)
- pacific-norfolk - (GMT+11:30) Norfolk Island
- pacific-samoa (GMT-11:00; Samoa)
- us-alaska (GMT-9:00; Alaska)
- us-arizona (GMT-7:00; Arizona)
- us-central (GMT-6:00; Chicago, Mexico City, Saint Louis)
- us-eastern (GMT-5:00; Bogota, Lima, New York City)
- us-hawaii (GMT-10:00; Hawaii)
- us-indiana (GMT-6:00; Indiana)
- us-mountain (GMT-7:00; Cheyenne, Denver, Las Vegas)
- us-pacific (GMT-8:00) San Francisco, LA, Seattle
- utc (GMT; Universal Time Coordinated: London, Dublin, Edinburgh, Lisbon, Reykjavik, Casablanca)
**local**

Indicates the timezone specified by \( tz \) is to be considered the local time zone for local time display and conversion.

---

**Usage**

Clock and timezone management is necessary for proper accounting records. The chassis may be set to display a different local time than that of the system clock which allows accounting records to use the system time but to display the proper local time for users.

---

**Example**

```
clock timezone utc

clock timezone us-indiana local

no clock timezone
```
congestion-control

Enables/disables congestion control support on the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
congestion-control policy
default congestion-control
no congestion-control
```

- **default**
  Sets the congestion control to its default value.

- **no**
  Disables congestion-control functionality. This is the default setting.

**Usage**

Congestion control on the system is used to monitor the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (i.e., high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may impact the system’s ability to service subscriber sessions. The purpose of congestion control is to aid in the identification of such conditions and invoke policies for addressing the situation.

Congestion control operation is based on the configuration of the following:

- **Congestion condition thresholds:** Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.

A threshold tolerance is configured to dictate the percentage under the configured threshold that must be reached in order for the condition to be considered “cleared”. An SNMP trap (starCongestionClear) is then triggered.

- **Service congestion policies:** Congestion policies are configurable for each service (PDSN, GGSN, or HA). These policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Because congestion control functionality on the system is disabled by default, this command should be executed once congestion-control thresholds and policies have been configured. (Refer to the `congestion-control policy` and `congestion-control threshold` commands for more information.)
congestion-control overload-disconnect

This command enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.

To verify the congestion-control configuration use `show congestion-control configuration` from the Exec mode.

To set overload-disconnect policies for individual subscribers., see `overload-disconnect` in Subscriber Configuration Mode Commands.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
congestion-control overload-disconnect [ iterations-per-stage integer | percent percentage_value| threshold { license-utilization percentage_value | max-sessions-per-service-utilization percentage_value | tolerance number } ]

default congestion-control overload-disconnect [ iterations-per-stage | percent | threshold { license-utilization | max-sessions-per-service-utilization | tolerance } ]

no congestion-control overload-disconnect
```

- `iterations-per-stage integer`:
  An integer between 2 and 8. This value defines the number of calls to be disconnected during the defined number of seconds. The default value for this keyword is 8.

- `percent percentage_value`:
  An integer between 1 and 100 specifies the percentage of calls to be disconnected, in stages, during an overload situation. The default value is 5.

- `threshold`:
  - `license-utilization`: An integer value between 1 and 100 that specifies the license-utilization percentage threshold for overload situations. If candidates are available, passive calls are disconnected when this threshold is exceeded. The default value is 80.
  - `max-sessions-per-service-utilization`: An integer value between 1 and 100 that specifies a percentage of the maximum sessions per service. If candidates are available, passive calls are disconnected when this threshold is exceeded. The default value is 80.
  - `tolerance`: An integer between 1 and 25 that specifies the percentage of calls the system disconnects below the values set for the other two thresholds. In either case, a Clear Traps message is sent after the number of calls goes below the corresponding threshold value. The tolerance default value is 10.

- `default`:
  When ‘default’ and one of the keywords is added to the command, then the policy remains in its current state and the value for the specified keyword is reset to its default value.
When ‘default’ and the command are entered without keywords, then the overload-disconnect policy for congestion control is disabled.

```
no congestion-control overload-disconnect
```
Disables the overload-disconnect policy for congestion control.

**Usage**
Use this command to set the policy for call disconnects when the chassis experiences call overload.

**Example**
The following command sets an overload-disconnect policy for the chassis in which 5 calls would be disconnected very 5 seconds during an overload situation.

```
congestion-control overload-disconnect interactions-per-stage 5
```
Both of the following commands disable the overload-disconnect policy without changing the policy configuration.

```
default congestion-control overload-disconnect
```
or

```
no congestion-control overload-disconnect
```
To instruct the system to stop call disconnects when the number of calls goes down 85% of the total allowed calls for that service, enter both of the following commands to set the max-sessions-per-service-utilization value to 90% and the tolerance value to 5%:

```
congestion-control overload-disconnect threshold max-sessions-per-service-utilization 90
congestion-control overload-disconnect threshold tolerance 5
```
congestion-control policy

Configures congestion control policies.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default congestion-control policy {asngw-service | asnpc-service | ggsn-service | ha-service | lns-service | mipv6ha-service | pdsn-service pdg-service | pdif-service | sgsn-service}
```

### default congestion-control policy service
Sets the congestion policy action for the selected service to its default value.

### asngw-service
Sets the congestion policy action for the ASN GW service.

### asnpc-service
Sets the congestion policy action for the ASN PC-LR service.

### cscf-service
Sets the congestion policy action for the CSCF service.

### ggsn-service
Sets the congestion policy action for the GGSN service.

### ha-service
Sets the congestion policy action for the HA service.

### lma-service
Sets the congestion control policy action for the LMA service

### lns-service
Sets the congestion policy action for the LNS service.

### mipv6ha-service
Sets the congestion policy action for the MIPv6-HA service.

### mme-service
Sets the congestion control policy for action to take when subscriber sessions exceeds the defined threshold limit.
For MME type of session/calls redirect action is not supported.

**pdg-service**
Sets the congestion policy action for the PDG service.

**pdif-service**
Sets the congestion policy action for the PDIF service.

**pdsn-service**
Sets the congestion policy action for the PDSN service.

**sgsn-service**
Sets the congestion policy action for the SGSN service.

**action { drop | none | redirect | reject }**
Defines what policy action is taken:

- **drop**: Specifies that the system is to drop incoming packets containing new session requests. (PDSN, GGSN, ASN GW, LMA, MME, and ASN PC and HA only)
- **none**: Specifies that the system is take no action. This is the default for PDIF-service.
- **redirect**: Specifies that the system is to redirect new session requests to an alternate device. (PDSN and HA only)

**Important**: If this option is used, the IP address of the alternate device must be configured using the policy overload redirect command that is part of the service configuration. Note that this option can not be used in conjunction with GGSN and MME services.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message. (For PDSN and HA, the reply code is 130, “insufficient resources”. For the GGSN, the reply code is 199, “no resources available”.)

**Usage**
Congestion policies can be configured for each service. When congestion control functionality is enabled, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

**Example**
The following command configures a congestion control policy of reject for PDSN services:

```
congestion-control policy pdsn-service action reject
```

The following command configures a congestion control policy of reject for MME services:

```
congestion-control policy mme-service action reject
```
congestion-control threshold

Configures the congestion control threshold values that are to be monitored.

Product
All

Privilege
Security Administrator, Administrator

Syntax

congestion-control threshold { license-utilization percent | max-sessions-per-service-utilization percent | message-queue-utilization percent | message-queue-wait-time time | port-rx-utilization percent | port-specific { slot/port | all } [ tx-utilization percent ] [ rx-utilization percent ] | port-tx-utilization percent | service-control-cpu-utilization percent | system-cpu-utilization percent | system-memory-utilization percent | tolerance percent }


no congestion-control threshold port-specific { slot/port | all }

no congestion-control threshold port-specific { slot/port | all } [ rx-utilization percent ] [ tx-utilization percent ]

no congestion-control threshold { message-queue-utilization | message-queue-wait-time | port-rx-utilization percent | port-tx-utilization percent | service-control-cpu-utilization | system-cpu-utilization | system-memory-utilization }

default congestion-control threshold keyword
Sets the threshold keyword to its default value.

no congestion-control threshold port-specific { slot/port | all }
This command disables port specific threshold monitoring on the specified port or on all ports.

slot/port: Specifies the port for which port specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.

all: Set port specific threshold monitoring for all ports on all cards.

license-utilization percent
Default: 100
The percent utilization of licensed session capacity as measured in 10 second intervals.

percent can be configured to any integer value from 0 to 100.

max-sessions-per-service-utilization percent
Default: 80
The percent utilization of the maximum sessions allowed per service as measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the bind command for the PDSN, GGSN, SGSN, or HA services.) percent can be configured to any integer value from 0 to 100.

**message-queue-utilization** *percent*

Default: 80
The percent utilization of the Demux Manager software task’s message queue as measured in 10 second intervals. The queue is capable of storing a maximum of 10000 messages. percent can be configured to any integer value from 0 to 100.

**message-queue-wait-time** *time*

Default: 5
The maximum time (in seconds) messages can be held in queue as measured by packet time stamps. time is measured in seconds and can be configured to any integer value from 1 to 30.

*Important:* In the event that this threshold is crossed, an SNMP trap is not triggered. In addition, the service congestion policy invocation resulting from the crossing of this threshold is enforced only for the packet that triggered the action.

**[no]** **port-rx-utilization** *percent*

Default: 80
The average percent utilization of port resources for all ports by received data as measured in 5 minute intervals. percent can be configured to any integer value from 0 to 100.

**[no]** **port-specific** *(slot/port | all)* **[rx-utilization** *percent]* [**tx-utilization** *percent]*

Default: Disabled
Sets port-specific thresholds. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide. *slot/port*: Specifies the port for which port-specific threshold monitoring is being configured. The slot and port must refer to an installed card and port. *all*: Set port specific threshold monitoring for all ports on all cards. *rx-utilization* *percent*: Default 80%. The average percent utilization of port resources for the specified port by received data as measured in 5 minute intervals. percent must an integer from 0 through 100. *tx-utilization* *percent*: Default 80%. The average percent utilization of port resources for the specified port by transmitted data as measured in 5 minute intervals. percent must be an integer from 0 through 100.

**[no]** **port-tx-utilization** *percent*

Default: 80
The average percent utilization of port resources for all ports by transmitted data as measured in 5 minute intervals. percent can be configured to any integer value from 0 to 100.
Global Configuration Mode Commands

congestion-control threshold

Default: 80
The average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10 second intervals.
percent can be configured to any integer value from 0 to 100.

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01

system-cpu-utilization percent

Default: 80
The average percent utilization for all PSC/PSC2 CPUs available to the system as measured in 10 second intervals.
percent can be configured to any integer value from 0 to 100.
This threshold setting can be disabled with no congestion-control threshold system-cpu-utilization command. In case later you want to enable the same threshold setting congestion-control threshold system-cpu-utilization command will enable the CPU utilization threshold to preconfigured level.

system-memory-utilization percent

Default: 80
The average percent utilization of all CPU memory available to the system as measured in 10 second intervals.
percent can be configured to any integer value from 0 to 100.

tolerance percent

Default: 10
The percentage under a configured threshold that dictates the point at which the condition is cleared.
percent is an integer value from 0 to 100.

Usage

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.
The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap (starCongestionClear) is generated for the clear condition, as well.

Example

The following command configures a system CPU utilization threshold of 75%.
congestion-control threshold system-cpu-utilization 75
This setting will remain in configuration unless you specify another threshold value in place of 75. This threshold setting can be disabled with no congestion-control threshold system-cpu-utilization command but can not be removed from configuration. Later if you want to enable the previously configured threshold value of 75 percent you only need to enter congestion-control threshold system-cpu-utilization command without specifying any threshold value and it will enable the CPU utilization threshold to preconfigured level of 75 percent.
For example, no congestion-control threshold system-cpu-utilization will disable the configured threshold setting and congestion-control threshold system-cpu-utilization will again enable the threshold setting of 75%.
The following command configures a threshold tolerance of 5%:

```
congestion-control threshold tolerance 5
```

In the above examples, the starCongestion trap gets triggered if the system CPU utilization goes above 75% and the starCongestionClear trap gets triggered if it reaches or goes below 70%.
content-filtering category database directory

This command configures the base directory to be used for storing all content-rating databases that are required for Category-based Content Filtering application.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
content-filtering category database directory path directory_path
```

```
default content-filtering category database directory path
```

**default**
Specifies the default base directory and directory path for Category-based Content Filtering application.

**directory_path**
Default: /pcmcia1/cf
Specifies the base directory and its path to store all of the full or incremental content rating databases for the Category-based Content Filtering application.

directory_path must be an alpha and/or numeric string of 1 through 255 characters in length.

**Usage**
Use this command to specify the directory and its path to download all full or incremental category-rating databases to be used for the Category-based Content Filtering application.
Merging of incremental database can be done as part of the database upgrade process preformed with upgrade content-filtering category database command in the Executive Mode.

**Example**
The following command configures the /flash/cf_temp/DB as base directory to download all full and incremental content-rating databases for content filtering application.

```
content-filtering category database directory path /flash/cf_temp/DB
```
content-filtering category database max-versions

This command configures the number of full content-rating databases to maintain/archive in the base directory for category-based content filtering application.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
content-filtering category database max-versions num_archive

default content-filtering category database max-versions
```

- **default**
  Sets the default number of full databases for specified directory path/location.

- **num_archive**
  Default: 2
  Specifies the maximum number of database to be archived or maintained in the specific location.
  num_archive must be an integer between 1 and 3.

**Usage**
Use this command to set the number of full content-rating database to be maintained in the specified directory path with the base file name specified using the `content-filtering database override file` command. Note that the specified directory path is the location specified using the `content-filtering category database directory path` command.

**Example**
The following command configures the system to maintain 3 full content-rating databases for category-based content filtering application.

```
content-filtering category database max-versions 3
```
content-filtering category database override

This command specifies the name of a file to be used by the category-rating database load process for category-based content filtering application.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

content-filtering category database override file file_name.extension

default content-filtering category database override file

default
Sets the default content rating database file name; i.e. optcmd.bin.

file file_name.extension
Specifies the header of the file in the database directory path location to determine the newest full database. file_name must be an alpha and/or numeric string of up to 10 characters with an extension of 3 character after a period (.) as extension.

Usage
Use this command to configure the category-rating database file name to determine the newest version of full database. A process called “LOAD_DATABASE” invokes during the system startup or the database upgrade process by upgrade content-filtering category database command in Executive Mode. This process examines the header of each of the files in the database folder specified by content-filtering category directory path command in this mode. Note that by default system examines the header of those files only which begins with the string “OPTCMDB” and having extension “.bin”.

Example
The following command configures the system to examine the header of files that begins with CF_sta.DB only for content filtering application.

content-filtering category database override file CF_sta.DB
context

Enters the context configuration mode or is used to add or remove a specified context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

context name[ -noconfirm ]

no context name

no
Removes the specified context from the configuration.

name
Specifies the name of a context to enter, add, or remove. When creating a new context, the context name must be unique, it may not be the same as any existing context or any domain specified within any context.

Important: When creating a new context, the context name specified must not conflict with the name of any existing context or domain names.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Configure contexts or remove obsolete contexts.

Important: A maximum of 64 contexts may be created.

Example

context sampleContext

no context sampleContext
crash enable

Enables/disables the copying of crash data to a specified location.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
crash enable [ encrypted ] url crash_url [ filename-pattern pattern ] [ restrict mbyte ]
```

```
no crash enable
```

no

Removes the specified context from the configuration.

**Important:** System crash information is generated and stored in the crash list even when the `no` keyword is specified. The information maintained in the crash lists is minimal crash information when the `no` keyword has been specified.

**encrypted**

The URL specified is in an encrypted format for security reasons.

**filename-pattern pattern**

The `filename-pattern` is a string containing any or all of the following variables:
- `%hostname%` - The system hostname.
- `%ip%` - A SPIO IP address
- `%cpu%` - CPU number
- `%card%` - Card number
- `%time%` - POSIX timestamp in hexadecimal notation
- `%filename%` - Alias for `crash-%card%-%cpu%-%time-core%`
- `%%` - A single % sign

If no pattern is specified the result is the same as the pattern `filename`. Use '/' characters in the filename pattern part to store crashes in per-system subdirectories.

**url crash_url**

Specifies the location to store crash files. `crash_url` may refer to a local or a remote file. `crash_url` must be entered using one of the following formats:
- `{file://[/flash]/pcmcia1[/pcmcia2][/directory]}/`
- `{tftp://[host[:port]]/[directory]}/`
- `{ftp://sftp://[username[:password]@] [host][:port]/[directory]}/`
Global Configuration Mode Commands

- ASR 5000:
  - file://flash/pcmcia1/hd[/directory]/
  - tftp://host[:port]//directory/ 

**Important:** Use of the SMC hard drive is not supported in this release.

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

restrict mbyte

Default: 128
Specifies a maximum amount of memory to use for storing crash files where mbyte is in megabytes and must be in the range from 1 through 128 megabytes.
The restrict keyword is only applicable to local URLs.

Usage
Enable crashes if there are systems that are not stable and the crash information will be useful for troubleshooting. The remote storage of the crash file reduces the memory utilized on the chassis.

Example

```
  crash enable ftp://remoteABC/pub/crash.dmp
  crash enable /flash/pub/data/crash.dmp restrict 64
  no crash enable
```
cs-network

This command creates/removes an HNB-CS network configuration instance for Femto UMTS access over Iu-CS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and CS networks elements; i.e. MSC/VLR. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

Product
HNB-GW

Privilege
Administrator

Syntax

```
 cs-network cs_instance [-noconfirm]
```

```
 no cs-network cs_instance
```

```
 no
 Removes the specified HNB-CS network instance from the system.
```

⚠️ Caution: Removing the HNB-CS network instance is a disruptive operation and it will affect all UEs accessing MSC(s) configured in specific CS core network through the HNB-GW service.

⚠️ Caution: If any HNB-CS Network instance is removed from system all parameters configured in that mode will be deleted and Iu-CS/Iu-Flex interface will be disabled.

```
 cs_instance
 Specifies the name of the Circuit Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN in HNB RN-PLMN configuration mode. If cs_instance does not refer to an existing HNB-PS network instance, the new HNB-CS network instance is created.
 cs_instance must be from 1 to 63 alpha and/or numeric characters.
```

```
 -noconfirm
 Indicates that the command is to execute without any additional prompt and confirmation from the user.
```

Usage

Use this command to enter the HNB-CS Network Configuration mode for an existing CS network instance or for a newly defined HNB-CS network instance. This command is also used to remove an existing HNB-CS network instance.

This configuration enables/disables the Iu-CS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.

A maximum of 8 HNB-CS network instance can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.
Caution: This is a critical configuration. The HNBs can not access MSC(s) in CS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to CS core network.

Entering this command results in the following prompt:

```
[context_name] hostname(config-cs-network)#
```

The various parameters available for configuration of an HNB-CS network instance are defined in the HNB-CS Network Configuration Mode Commands chapter of Command Line Interface Reference.

**Example**

The following command enters the existing HNB-CS Network configuration mode (or creates it if it doesn’t already exist) for the instance named *hnb-csl*:

```
cs-network hnb-csl
```

The following command will remove HNB-CS network instance *hnb-csl* from the system without any warning to operator:

```
no cs-network hnb-csl
```
css acsmgr-selection-attempts

This is a restricted command. In Release 9.0 and later, this command is obsoleted.
css delivery-sequence

This is a restricted command. In Release 9.0 and later, this command is obsoleted.
css service

This is a restricted command. In Release 9.0 and later, this command is obsoleted.
default

Restores the system default values for the specified parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

default { aaa { domain-matching | username-format } | autoconfirm | banner [ lawful-intercept | motd | pre-login ] | boot [ delay | interface | nameserver | networkconfig ] | card-standby-priority | cli max-sessions | congestion-control | logging { display | filter runtime } | operational-mode | pac-standby-priority | qos npu inter-subscriber traffic { bandwidth | priority{ assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } } } | require session recovery | snmp { engine-id |notif-threshold } | system hostname | task { facility sessmgr start | resource cpu-memory-low } | threshold { value } | timestamps | upgradelimit [ time ] [ usage] } 

aaa { domain-matching | username-format}

domain-matching - Resets the system to consider case when matching domains.
username-format - Resets the username format to the default of username @

autoconfirm

Restores the autoconfirm behavior to its default of disabled.

banner

lawful-intercept - Restores the system default message of the day for SSH CLI sessions.
motd - Restores the system default message of the day banner.
pre-login - Restores the CLI log in banner to the system default.

boot [delay | interface | nameserver | networkconfig]

interface | networkconfig - Restores the default boot interface and network configuration options. The keywords interface and networkconfig are used to restore the default option settings for the interface and network configuration options, respectively.

Defaulting the network configuration boot option removes the network boot option from the boot.sys file. It does not remove the network config options from the configuration file which is managed separately from the boot.sys file.
delay - Removes the boot delay setting (if any). The default for boot delay is “no boot delay”.
	nameserver - Removes the nameserver IP address.

card-standby-priority

Restets the standby priority of the Packet Services Cards.
cli max-sessions
Restores the default value of this command to no cli max-sessions which removes the limit on the number of allowed simultaneous CLI sessions on the system.

congestion-control
Restores the system’s congestion-control functionality to its default setting of disabled.

logging {display | filter runtime}
display: sets the default level of detail to display for trace log information to the system default.
filter runtime: resets the filtering of logged information to log in real time.

operational-mode
Sets the operational mode of the chassis to the system default.

pac-standby-priority
This parameter has been replaced by the card-standby-priority keyword.

qos npu inter-subscriber traffic {bandwidth | priority [ assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } ] }
Restores the following NPU QoS parameters to their default values:
  * bandwidth:
  * gold: 10%
  * silver: 20%
  * bronze: 30%
  * best-effort: 40%
  * priority: All DSCP values are mapped to the best-effort priority queue but are not configured.

require session recovery
 Resets the session recovery feature to its default setting of disabled.

snmp { engine-id | notif-threshold | system hostname | timestamps }
engine-id: restores the SNMP engine ID to the system default.
notify-threshold: restores the SNMP notification threshold to the system default.

task { facility sessmgr start | resource cpu-memory-low }
facility sessmgr start: Restores the default session manager start policy.
resource cpu-memory-low: Resets the system so that when a CPU runs very low on memory (below 12MB) the most over limit task is killed.

system hostname
Sets the system host name for SNMP use to the system default value.
threshold { value }

Restores thresholding values to their default setting. The possible values are:

- **10sec-cpu-utilization**: CPU utilization using a 10 sec average.
- **aaa-acct-failure**: AAA accounting failure threshold settings
- **aaa-acct-failure-rate**: AAA accounting failure rate threshold settings
- **aaa-auth-failure**: AAA authentication failure threshold settings
- **aaa-auth-failure-rate**: AAA authentication failure rate threshold settings
- **aaa-retry-rate**: AAA retry rate threshold settings
- **call-reject-no-resource**: Calls rejected due to no resources threshold settings
- **call-setup**: Calls setup threshold settings
- **call-setup-failure**: Call setup failure threshold settings
- **cpu-available-memory**: CPU available memory threshold settings
- **cpu-load**: PSC/PSC2 CPU load using a 5 minute average measurement
- **cpu-memory-usage**: Percentage of total CPU memory usage
- **cpu-session-throughput**: CPU session throughput threshold settings
- **cpu-utilization**: CPU utilization threshold settings
- **license**: Session license threshold settings
- **model**: Thresholding model settings
- **monitoring**: Threshold monitoring configuration settings
- **packets-filtered-dropped**: Filtered/dropped packet threshold settings
- **packets-forwarded-to-cpu**: Forwarded packet threshold settings
- **pdif-current-sessions**: Threshold monitoring for all current PDIF sessions.
- **pdif-current-active-sessions**: Threshold monitoring for only the currently-active PDIF sessions.
- **per-service-ggsn-sessions**: The number of GGSN sessions per GGSN service
- **per-service-gprs-sessions**: The number of GPRS sessions per GPRS service
- **per-service-gprs-pdp-sessions**: The number of PDP contexts per GPRS service
- **per-service-ha-sessions**: The number of HA sessions per HA service
- **per-service-kins-sessions**: The number of LNS sessions per LNS service
- **per-service-pdsn-sessions**: The number of PDSN sessions per PDSN service
- **per-service-sgsn-sessions**: The number of SGSN sessions per SGSN service
- **per-service-sgsn-pdp-sessions**: The number of PDP contexts per SGSN service
- **poll**: Threshold polling interval configuration settings
- **total**: Total subscriber threshold settings
- **total-ggsn-sessions**: Total GGSN sessions for all GGSN services in the system
- **total-gprs-sessions**: Total GPRS sessions per for all GPRS services in the system
- **total-gprs-pdp-sessions**: Total PDP contexts for all GPRS services in the system
- **total-ha-sessions**: Total HA sessions for all HA services in the system
Global Configuration Mode Commands

**default**

- **total-lns-sessions**: Total LNS sessions for all LNS services in the system
- **total-pdsn-sessions**: Total PDSN sessions for all PDSN services in the system
- **total-sgsn-sessions**: Total SGSN sessions per for all SGSN services in the system
- **total-sgsn-pdp-sessions**: Total PDP contexts for all SGSN services in the system

**timestamps**

Resets the inclusion of timestamps in command.

**upgrade limit [ time ] [ usage ]**

Sets upgrade limit values to the defaults. If the optional keywords are not specified all values are reset to their defaults.

- **time**: Resets the maximum time a session may exist during a software upgrade to the default of 120.
- **usage**: Resets the minimum number of sessions before closing the sessions during a software upgrade to the system default of 100.

**Usage**

Restore system defaults to aid in trouble shooting or just prior to modifying additional configuration options.

**Example**

- default banner motd
- default boot
- default logging display
- default system hostname
- default upgrade limit time
diameter-proxy ram-disk-limit

This command configures the amount of extra RAM disk space in MB to be allocated to Diamproxy task when local storage (hard disk) is enabled.

**Product**
SGW, PGW, HSGW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
diameter-proxy ram-disk-limit mb space_mb
default diameter-proxy ram-disk-limit mb
```

**default**
Confirms the default setting.
Default: 32 MB

**mb space_mb**
Specifies the storage space in MB.
`space_mb` must be an integer from 10 through 256.

**Usage**
Specifies the additional storage space to be allocated to Diamproxy for file write, in MB. The specified memory in MB is added to the existing memory allocated to Diamproxy only if HDD storage is enabled. By default, 32 MB is additionally allocated.

**Example**
The following command specifies that 100 MB of additional storage space be allocated to the Diamproxy task:

```
diameter-proxy ram-disk-limit mb 100
```
end

Exits the configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
enforce imsi-min equivalence

Enables the PDSN/HA to treat IMSI and MIN as the same for identifying the PDSN/HA session.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

enforce imsi-min equivalence

[ no | default ] enforce imsi-min equivalence

[ no | default ]
Disables the PDSN/HA from treating IMSI and MIN as the same for identifying the PDSN/HA session. Default: Disabled.

Usage
Generally on an HA, the IMSI and MIN are treated as different and hence the RRQs with 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session if the NAI and HoA also match. If the NAI and/or HoA do not match, then the duplicate IMSI session detect and terminate feature is applicable.

Generally on a PDSN, the IMSI and MIN are treated as different and hence RP messages from 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching PDSN sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session.

Example
To monitor or clear subscriber session information filtered by on IMSI/MIN refer to the show subscribers msid command.

Important: This command must be executed at startup only and will not take effect when reconfigured without rebooting.

Example
The following command enables the treatment of the IMSI and MIN as the same for identifying the session:

enforce imsi-min equivalence

Either of the following commands disables the treatment of the IMSI and MIN as the same for identifying sessions:
enforce imsi-min equivalence

no enforce imsi-min equivalence

default enforce imsi-min equivalence
**exit**

Exits the current mode, global configuration mode, and returns the CLI session to the previous mode, Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the Exec mode. This command has the same effect as the `end` command as the global configuration mode’s parent mode is the Exec mode.
**gtpp compression-process**

This command configures the maximum number of child compression processes that AAA proxy can have. This command is only applicable to the ASR 5000 platform.

**Product**

GGSN, SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
gtpp compression-process max_number

default gtpp compression-process
```

- **default**
  - Restores the system to the default settings for the number of child compression processes allowed.

- **max_number**
  - Specifies the maximum number of child processes. The default is 1
  - `max_number`: Must be an integer from 1 to 4.

**Usage**

This command configures the maximum number of child compression processes that AAA proxy can have only if hard disk storage is enabled.

**Example**

```
gtpp compression-process 3
```
**gtpp ram-disk-limit**

This command configures additional storage space to be allocated for writing files. This command is only applicable to the ASR 5000 platform.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp ram-disk-limit mb mega_bytes
default gtpp ram-disk-limit
```

- **default**
  Restores the system to the default settings of 32 MB of storage.

- **mb mega_bytes**
  Specifies the number of megabytes of storage allocated for files.
  `mega_bytes`: Must be an integer from 10 to 256. The default is 32 MB.

**Usage**
The memory specified with this command would be added to the existing memory allocated to the AAA proxy only if hard disk storage is enabled.

**Example**

```
gtpp ram-disk-limit mb 256
```
**gtpp single-source**

Configures the system to reserve a CPU for performing a proxy function for accounting.

**Product**
GGSN, SGSN, P-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp single-source [ centralized-lrsn-creation | private-extensions ]
no gtpp single-source
```

**centralized-lrsn-creation**
Defines the LRSN generation at proxy. The AAA proxy will generate the LRSN for all CDR types generated by either the GGSN or the SGSN.
Default: disabled

**private-extensions**
It is an optional keyword, enables the proprietary use of customer-specific GTPP extensions.
If `private-extensions` is not configured, all customer specific private extensions related to GTPP message transfer with CGF and recovery through GSS are disabled.

**Important:** In order for the customer-specific extensions to work properly, the `gtpp max-pdu-size` command in the Context Configuration Mode should be set to 65400 and the `gtpp server` command’s `max` value should be set to “1”.

```
no
```

Disables GTPP single-sourcing. This is the default setting.

**Caution:** Entering this command while PDP contexts are in process could cause the loss of pending CDRs. The configuration must be saved and the chassis reloaded for this option to take effect.

**Usage**
When GTPP single-sourcing is enabled, the system’s AAA proxy function generates requests to the accounting server using a single UDP source port number, instead of having each AAA Manager generate independent requests with unique UDP source port numbers. This is accomplished by the AAA Managers forwarding their GTPP PDUs to the AAA Proxy function that runs on a reserved PSC/PSC2 CPU. Since a PSC/PSC2 CPU is being reserved, fewer Session Managers and AAA Managers will be started on that PSC.

**Caution:** This command must be entered prior to the configuration of other services. Specifying it later may return an error due to a lack of CPU availability.
Example

The following command enables GTPP single-sourcing with the use of private GTPP extensions:

```
gtp single-source private-extensions
```

The following command disables GTPP single-sourcing:

```
no gtp single-source
```
**global-title-translation address-map**

Creates an instance of a Global Title Translation (GTT) address-map, a database, for global titles (ISDN-type address) used for SCCP routing. Upon creating the instance, the system enters global title translation address-map configuration mode. For the commands to configuration the database, go to the Global Title Translation Address-Map Configuration Mode chapter in this guide.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
global-title-translation address-map name
no global-title-translation address-map name
```

- **no**
  Removes the specified GTT address-map database from the SCCP portion of the configuration.

- **name**
  This value uniquely identifies a specific instance of a GTT address-map.
  `name`: must be a string of 1 to 63 alphanumeric characters.

**Usage**
Create a GTT address-map with a unique identifier and enter the GTT address-map configuration mode.

**Example**

```
global-title-translation address-map gtt-map1
```
**global-title-translation association**

Creates an instance of a Global Title Translation (GTT) association which defines the rules for handling global title translation. Upon creating the instance, the system enters global title translation association configuration mode. For the commands to configure the rules, go to the Global Title Translation Association Configuration Mode chapter in this guide.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
global-title-translation association name

no global-title-translation association name
```

no

Removes the specified instance of a GTT association from the SCCP portion of the configuration.

name

This value uniquely identifies a specific instance of a GTT association. 
name: must be a string of 1 to 63 alphanumeric characters.

**Usage**

Create a GTT association with a unique identifier and enter the GTT association configuration mode.

**Example**

```
global-title-translation association gtt-asscl
```
hd raid

Provides access to a local RIAD hard drive configuration mode in order to manage parameters supporting local storage of records.

Product
All

Privilege
Security Administrator, Administrator

Syntax

hd raid

raid
Provides access to the HD RAID configuration mode in order to manage the RAID on the ASR 5000 SMC hard drive.

Usage
Enters the HD RAID configuration mode.
Entering this command results in the following prompt:

[context_name]hostname(config-hd-raid)#

HD RAID Configuration Mode commands are defined in the HD RAID Configuration Mode Commands chapter.

Example
The following command opens the hd-raid mode:

hd raid
hd storage-policy

Provides access to the local hard drive configuration mode in order to manage parameters supporting local storage of records.

Product
GGSN, SGSN, HSGW, P-GW, S-GW

Privilege
Administrator

Syntax

**hd storage-policy name**

**no hd storage-policy name**

**no**
Removes a configured HD storage policy from the system.

**storage-policy name**
Specifies a name for an HD storage policy and enters the HD Storage Policy Configuration Mode. *name* must be from 1 to 63 alpha and/or numeric characters.

Usage
Creates a new policy or specifies an existing policy and enters the HD Storage Policy Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-hd-storage-policy)#
```

HD Storage Policy Configuration Mode commands are defined in the HD Storage Policy Configuration Mode Commands chapter.

Example
The following command creates an HD storage policy named *policy3* and enters the HD Storage Policy Configuration Mode:

```
hd storage-policy policy3
```
high-availability

Configures PSC/PSC2 task failure detection speed.

Product
PDSN, GGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax

```
high-availability fault-detection speed { aggressive | normal }
default high-availability fault-detection speed

{ aggressive | normal
Default: normal
• aggressive: Initiates PSC failover without performing additional checks.
• normal: Initiates PSC failover after additional checks are performed.
```

Usage

Use this command to increase the fault detection speed for faster switchovers after a PSC/PSC2 task failure. Setting fault detection speed to aggressive will trigger PSC/PSC2 failover as soon as possible if a potential failure is detected. Aggressive mode will reduce the duration of subscriber outages caused by a failed PSC/PSC2 if session recovery is enabled.

Aggressive mode also bypasses most information gathering steps and logs that can be used to determine the root cause of the failure.

In normal mode, additional checks are performed before triggering a PSC/PSC2 failover to ensure the card has actually failed. In aggressive mode these checks are bypassed so that session recovery can start as soon as possible. These additional checks reduce the likelihood of a false positive failure.

Example

The following command sets the fault detection speed for PSC/PSC2/tasks to aggressive:

```
high-availability fault-detection speed aggressive
```
license

Configures the session license key.

Product
All

Privilege
Security Administrator, Administrator

Syntax

license key key_value [ -force ] session-limit

no license key key_value [ -force ] session-limit

no
Removes the license key(s) installed.

key key_value
Installs the license key specified by key_value. key_value is provided by Cisco Systems operations staff.

session-limit
Use this keyword to suppress fail-over calls from being rejected if the licensed threshold is crossed.

**Important:** This is a customer-specific command that is available for HA, PDSN, EHA, and PDIF. Please contact your local sales representative for more information.

-force
Sets the license key even if resources are not available. The system supports the dynamic resizing of demultiplexor software tasks based on the licensed session capacity and feature type. When installing a license, the system automatically attempts to resize currently functioning tasks. Warning messages are displayed if there is an issue. Though it’s use is not recommended, the -force keyword can be used to suppress these warning messages.

**Caution:** Use of this option is not recommended.

Usage
Install or update system session keys when necessary due to expiration and/or capacity needs.

Example

license key sampleKeyValue
no license key
line

Enters the terminal display line configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
line
```

Usage
Change the terminal display configuration based upon the users own terminal characteristics.
local-user allow-aaa-authentication

Enables/disables the use of administrative accounts other than local-user administrative accounts.

Product
All

Privilege
Security Administrator, Administrator

Syntax

local-user allow-aaa-authentication
no local-user allow-aaa-authentication
default local-user allow-aaa-authentication

**no**
Disables administrative user accounts other than local-user accounts.

**default**
Returns this parameter to its default setting of enabled.

Usage
Local-user administrative accounts are separate from other administrative user accounts configured at the context level (Security Administrator, Administrator, Operator, and Inspector). Context-level administrative users rely on the system’s AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Since the T1.276-2003 password security mechanisms are supported only for local-user administrative accounts and not for the AAA-based administrative accounts, this command provides a mechanism for disabling AAA-based administrative accounts. By default, AAA-based administrative accounts are allowed.

Example
The following command forces the system to authenticate local-user accounts based only on the information in the security account file on its CompactFlash:

```
no local-user allow-aaa-authentication
```
local-user lockout-time

Configures the lockout period for local-user administrative accounts.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
local-user lockout-time time

default local-user lockout-time
```

**default**
Restores the parameter to its default setting.

**time**
Default: 60
The amount of time that must elapse before a previously locked-out local-user account can attempt to login again. *time* is measured in minutes and can be configured to any integer value between 1 and 10080.

**Usage**
Local-user administrative accounts can become locked for reasons such as exceeding the configured maximum number of login failures. Once an account is locked, this parameter specifies the lockout duration. Once the amount of time configured by this parameter has elapsed, the local-user can once again attempt to login.

**Example**
The following command configures a lockout time of 120 minutes (2 hours):

```
local-user lockout-time 120
```
**local-user max-failed-logins**

Configures the maximum number of failed login attempts a local-user can have before their account is locked out.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
local-user max-failed-logins number
no local-user max-failed-logins
default local-user max-failed-logins
```

- **no**
  Disables this functionality.

- **default**
  Restores this parameter to its default setting.

- **number**
  Default: 5
  Specifies the maximum number of times a local-user could experience a login failure before their account is locked out. number can be configured to any integer value between 2 and 100.

**Usage**
This command configures the maximum number of failed login attempts a local-user can have before their account is locked out. For example if, this parameter is configured to “3” then after the third failed login attempt, the account would be locked.

**Important:** Local-user accounts can be configured to either enforce or reject a lockout due to the maximum number of failed login being reached. Refer to the `local-user username` command for more information.

Refer to the `local-user lockout-time` command for more information.

**Example**
The following command configures a maximum of three login attempts:

```
local-user max-failed-logins 3
```
local-user password

Configures local-user administrative account password properties.

Product
All

Privilege
Security Administrator, Administrator

Syntax

local-user password { [ complexity { ansi-t1.276-2003 | none } ] [ history length number [ duration days ] ] [ max-age days ] [ min-change-char number ] [ min-change-interval days ] [ min-length number ] }

no local-user password { [ history ] [ max-age ] [ min-change-interval ] }

default local-user password { [ complexity ] [ history ] [ max-age ] [ min-change-char ] [ min-change-interval ] [ min-length ] }

---

no

Disables the specified parameter.

default

Restores the specified parameter to its default setting.

[ complexity { ansi-t1.276-2003 | none } ]

Default: ansi-t1.276-2003
Specifies the password strength as one of the following:

• ansi-t1.276-2003: If this option is selected, then the following rules are enforced:
  • Passwords may not contain the username or the reverse of the username
  • Passwords may contain no more than 3 of the same characters used consecutively
  • Passwords must contain at least three of the following:
    • upper case alpha character
    • lower case alpha character
    • numeric character
    • special character
• none: No additional password checks are performed.

[ history length number [ duration days ] ]

Default: length is 5
Specifies the number of previous password entries kept in the history list maintained by the system. A password can not be reused if it is one of the entries kept in the history list unless the time it was last used was more than the number of days specified by the duration keyword.
If the duration keyword is not used, the only check performed by the system is that it is not in the history list.
**local-user password**

`number` is the number of entries for each account stored in the history list and can be configured to any integer value from 1 to 100. `days` is the number of days during which a password can not be reused and can be configured to any integer value between 1 and 365.

```
[ max-age days ]
Default: 90
Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. Once the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI.
```

**Important:** Local-user accounts can be configured to either enforce or reject a lockout due to a password’s maximum age being reached. Refer to the `local-user username` command for more information.

`days` is the number of days that passwords remain valid and can be configured to any integer value from 1 to 365.

```
[ min-change-char number ]
Default: 2
Specifies the minimum number of characters that must be changed (in comparison to the current password) when a user changes their password.
```

**Important:** Changes in password length are counted as “character” changes. For example: changing a password from “password” to “passwo” is a 2-character change, changing a password from “password” to “password2” is a 1-character change, and changing a password from “password” to “apassword” is a 9-character change.

`number` is the number of characters and can be configured to any integer value between 0 and 16.

```
[ min-change-interval days ]
Default: 1
Specifies the frequency that passwords can be changed (other than first login).
`days` is the minimum number of days that must pass before a user can change their password. It can be configured to any integer value from 1 to 365.
```

**Important:** If the `no local-user password min-change-interval` command is used, users may change their password as often as desired which could allow them to circumvent the password history function.

```
[ min-length number ]
Default: 8
Specifies the minimum length allowed for user-defined password.
`number` is the minimum number of alpha and/or numeric characters that the password must contain and can be configured to any integer value between 3 and 32.
```

**Usage**

This command is used to set the property requirements for user-defined passwords and system behavior in relation to those passwords.
Information pertaining to user passwords, login failures, and password history are stored on the SMC’s CompactFlash and in the software’s Shared Configuration Task (SCT). The system uses the information in SCT for runtime operations such as determining password ages and determining if new passwords meet the criteria specified by this command.

**Example**
The following command configures a minimum password length requirement of 6 characters:

```plaintext
local-user password min-length 6
```

The following command configures the system to store the 4 most recently used passwords per user-account in the history list:

```plaintext
local-user password history length 4
```
local-user username

Adds/removes local-user administrative accounts.

Product
All

Privilege
Security Administrator, Administrator

Syntax

local-user username name [ authorization-level { administrator | inspector | operator | security-admin } ] [ ecs | noecs ] [ ftp | noftp ] [ timeout-min-absolute time ] [ timeout-min-idle time ] [ no-lockout-login-failure ] [ no-lockout-password-aging ] password password

no local-user username

no
Removes a previously configured user.

name
Specifies the name of the user. The name must be from 3 to 16 alpha and/or numeric characters in length and is case sensitive.

[ authorization-level { administrator | inspector | operator | security-admin } ]

Default: Operator

Configures the authorization level for the user as one of the following:

• administrator: Administrator users have read-write privileges and can execute any command throughout the CLI except for a few security functions allowed only in the administrator mode. Administrators can configure or modify the system and are able to execute all system commands, including those available to the operator and inspector user. This level corresponds to the both the System Administrator and Application Administrator levels in T1.276-2003.

• inspector: Inspector users are limited to a small number of read-only Exec Mode commands. The bulk of these are “show” commands giving the inspector the ability to view a variety of statistics and conditions. The Inspector cannot execute show configuration commands and do not have the privilege to enter the Config Mode.

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

• security-admin: Security Administrator users have read-write privileges and can execute any command throughout the CLI. Security Administrators can execute all system commands, including those available to the administrator, operator, and inspector users. This level corresponds to both the System Security Administrator and Application Security Administrator levels in T1.276-2003.
[ ecs | noecs ]
Default: ecs
Specifies whether or not the user has access to configuration parameters pertaining to the Enhanced Charging Service.

- ecs: The user has access.
- noecs: The user does not have access.

[ ftp | noftp ]
Default: ftp
Specifies whether or not the user is allowed to access the system via the File Transfer Protocol (FTP) and/or the Secure File Transfer Protocol (SFTP).

- ftp: The user has access.
- noftp: The user does not have access.

[ timeout-min-absolute time ]
Default: 0
Specifies the maximum session time for this user. time is measured in minutes and can be configured to any integer value between 0 and 525600. A value of “0” indicates no limit.

**Important:** This limit applies only to the user’s CLI sessions.

[ timeout-min-idle time ]
Default: 0
Specifies the maximum idle time for this user. time is measured in minutes and can be configured to any integer value between 0 and 525600. A value of “0” indicates no limit.

**Important:** This limit applies only to the user’s CLI sessions.

[ no-lockout-login-failure ]
Default: Disabled
Specifies that this user will never be locked out due to login attempt failures.

[ no-lockout-password-aging ]
Default: Disabled
Specifies that this user will never be locked out due to the age of their password.

**password** password
Specifies the initial password for this user. password must from 6 to 32 alpha and or numeric characters in length and is case sensitive.

**Important:** The user is requested to change their password upon their first login.

**Usage**
The ability to configure administrative local-users is provided in support of the login security mechanisms specified in ANSI T1.276-2003. Like administrative users configured at the context level, local-users can be assigned one of 4 security levels:

<table>
<thead>
<tr>
<th>Local-User Level User</th>
<th>Context Level User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Administrator</td>
<td>Administrator</td>
</tr>
<tr>
<td>Administrator</td>
<td>Config-Administrator</td>
</tr>
<tr>
<td>Operator</td>
<td>Operator</td>
</tr>
<tr>
<td>Inspector</td>
<td>Inspector</td>
</tr>
</tbody>
</table>

Local-user configuration support is handled differently from that provided for administrative users configured at the context level. Context-level administrative users rely on the system’s AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Passwords for these user types are assigned once and are accessible in the configuration file. Local-user account information (passwords, password history, lockout states, etc.) is maintained in non-volatile memory on the CompactFlash module and in the software’s Shared Configuration Task (SCT). This information is maintained in a separate file—not in configuration files used by the system. As such, the configured local-user accounts are not visible with the rest of the system configuration. Local-user and context-level administrative accounts can be used in parallel.

Example

The following command configures a security-administrator level local-user administrative account for a user named User672 that has FTP privileges, a temporary password of abc123, and that does not lockout due to either login attempt failures or password aging:

```
local-user username User672 authorization-level security-admin ftp no-lockout-login-failure no-lockout-password-aging password abc123
```

The following command deletes a previously configured local-user administrative account called admin32:

```
no local-user username admin32
```
logging

The commands in this section set logging parameters.
logging console

Enables the output of logged events to be displayed on the console terminal.

Product
All

Privilege
Security Administrator, Administrator

Syntax
logging console

no logging console

Usage
Log console output to allow for offline review during system monitoring and/or trouble shooting.
logging disable

Enables/disables the logging of the specified event ID or range of IDs.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
logging disable eventid id [ to to_id ]
```

```
no logging disable eventid id [ to to_id ]
```

- `no`
  Indicates the event IDs specified are to be enabled for logging.

- `eventid id`
  Specifies the event for which no logging is to occur. `id` must be a value in the range 1 through 100000.

- `to to_id`
  Specifies the end ID of the events when a range of event ID is to be disabled from being logged. `to_id` must be a value in the range 1 through 100000. The `to_id` must be equal to or larger than the `id` specified.

**Usage**

Disable common events which may occur with a normal frequency are not of interest in monitoring the system for troubles.

**Example**
The following commands disables the logging of event ID 4580 and the range of events from 4500 through 4599, respectively.

```
logging disable eventid 4580

logging disable eventid 4500 to 4599
```

The following enables the subset of disabled event IDs:

```
no logging disable eventid 4500 to 4549
```
logging display

Configures the level of detail for information to be logged.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
logging display [ event-verbosity evt_level ] [ pdu-dataformat ] [ pdu-verbositypdu_level ]
```

---

event-verbosity evt_level

Specifies the level of verboseness to use in logging of events as one of:
- min
- concise
- full

---

pdu-data format

Specifies output format for packet data units when logged as one of:
- none
- hex
- hex-ascii

Where none results in the output in raw format, hex results in the output being displayed in hexadecimal format, and hex-ascii results in the output being displayed in hexadecimal and ASCII similar to a main-frame dump.

---

pdu-verbosity pdu_level

Specifies the level of verboseness to use in logging of packet data units as a value from 1 to 5 where 5 is the most detailed.

---

**Usage**

Tune the level of information to be logged so as to avoid flooding a log file with information which is not useful or critical.

---

**Example**
The following sets the logging display for events to the maximum.

```
logging display event-verbosity full
```

The following command sets the logging display level of detail for packet data units to level 3 and sets the output format to the main-frame style hex-ascii:
logging display pdu-data hex-ascii pdu-verbosity 3
logging filter

Configures the logging of events to be done in real time for the specified facility.

Product
All

Privilege
Security Administrator, Administrator

Syntax

logging filter runtime facility facility_level report_level [ critical-info | no-critical-info ]

facility facility

Specifies the facility to modify the filtering of logged information for as one of:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **acl-log**: Access Control List logging facility
- **acscrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **all**: All facilities
- **asf**: Voice Application Server Framework logging facility
- **asfprt**: ASF Protocol Task (SIP) logging facility
- **asngwmg**: ASN Gateway Manager facility
- **asnrmgr**: ASN Paging/Location-Registry Manager facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bssap**: Base Station Sub-system Application Part+ logging facility
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility
- **cap**: Camel Application Part logging facility
- **chatconf**: Voice Chat/Conference logging facility
- **cli**: CLI logging facility
- **credit-control**: Credit Control facility
- **cscf**: IMS/MMD CSCF
- **cscfmg**: SIP CSCF Manager facility
Global Configuration Mode Commands

- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **dcardctrl**: IPSEC Daughter card Controller logging facility (not used at this time)
- **dcardmgr**: IPSEC Daughter card Manager logging facility (Not used at this time)
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcpv6**: DHCPV6
- **dhcp**: DHCP facility (GGSN product only)
- **dhost**: Distributed Host logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-ecs**: ECS Diameter signaling facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSEC Data Path facility
- **drvctrl**: Driver Controller facility
- **ds3mgr**: DS3 Manager logging facility
- **eap-ipsec**: EAP
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface Logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Inline per-subscriber Stateful Firewall facility
- **gmm**: GMM Protocol logging facility
- **gprs-ns**: GPRS-NS Protocol logging facility
- **gss-gedr**: GTPP Storage Server GCDR facility
- **gtpe**: GTP-C protocol logging facility (GGSN product only)
- **gtpecmgr**: GTP-C protocol Manager logging facility (GGSN product only)
- **gtpp**: GTP-PRIME protocol logging facility (GGSN product only)
- **gtpu**: GTP-U protocol logging facility (GGSN product only)
- **h248pnt**: H.248 Protocol logging facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **igmp**: IGMP
- **ikev2**: IKEv2
Global Configuration Mode Commands

- **ims-authorizn**: IMS Authorization Service facility
- **ims-sh**: HSS SH Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipsec**: IP Security logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsps**: IP Pool Sharing Protocol logging facility
- **kvstore**: KV Store facility
- **l2tp-control**: L2TP control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **li**: Lawful intercept facility (Logs are visible only to system accounts with li-administrator privileges.)
- **linkmgr**: SGSN/SS7 Links Manager facility
- **llc**: Logical Link Control (LLC) Protocol logging facility
- **m3ua**: MTP3 User Adaptation (M3UA) Protocol logging facility
- **map**: Mobile Application Part (MAP) Protocol logging facility
- **megadiammgr**: Megadiameter Manager (SLF Service)
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 control logging facility
- **mtp3**: Message Transfer Part (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npumgr**: Network Processor Unit Manager facility
- **nsctrl**: Charging Service Controller facility (supported in conjunction with ECSv1)
- **nsmgr**: Charging Service Manager facility
- **nsproc**: Charging Service process facility
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF logging facility
- **pdif**: PDIF logging facility
- **pmm-app**: PMM application logging facility
- **ppp**: PPP link and packet facilities
- **ptt**: Voice push-to-talk logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: RANAP Protocol logging facility
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rip**: RIP logging facility (RIP is not supported at this time.)
- **rohc**: ROBust Header Compression facility
- **rsvp**: Reservation Protocol logging facility
- **sccp**: SCCP Protocol logging facility
- **sct**: Shared Configuration Task logging facility
- **sctp**: SCTP Protocol logging facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sft**: Switch Fabric Task logging facility
- **sgsn-app**: SGSN-APP interface logging facility
- **sgsn-gtpe**: SGSNs GTP-C Protocol logging facility
- **sgsn-gtpu**: SGSNs GTP-U Protocol logging facility
- **sgsn-misc**: SGSN miscellaneous logging facility
- **sgsn-system**: SGSNs System Components logging facility
- **sgsn-test**: SGSN Tests logging facility
- **sgtpcmgr**: SGSN GTPC Manager facility
- **sipcdprt**: Sip Call Distributor facility
- **sitmain**: System Initialization Task main logging facility
- **sm-app**: Session Management (SM) Protocol logging facility
- **sms**: Short Message Service (SMS) logging facility
- **sndcp**: Sub-Network Dependent Convergence (SNDCP) Protocol logging facility
- **snmp**: SNMP logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: Service Specific Co-ordination Function for UNNI (SCFNNI) Protocol logging facility
- **sscop**: Service Specific Connection Oriented Protocol (SSCOP) logging facility
- **ssh-ipse**: SSH IP Security logging facility
Global Configuration Mode Commands

- **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **taclcp**: Type Allocation Code (TAC) Local Call Processing logging facility
- **tcap**: Transaction Capabilities Application Part (TCAP) Protocol logging facility
- **threshold**: threshold logging facility
- **ttg**: TTG logging facility
- **tucl**: TUCL logging facility
- **udr**: User detail record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **vim**: Voice Instant Messaging logging facility
- **vinfo**: Voice Information logging facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6

```
level report_level [ critical-info | no-critical-info ]
```

**level report_level**: specifies the level of information to be logged, `report_level`, as one of:
- **critical**
- **debug**
- **error**
- **info**
- **trace**
- **unusual**
- **warning**.

**critical-info | no-critical-info**: indicates if critical information is to be displayed or not. The keyword **critical-info** specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. The **no-critical-info** keyword specifies that events with a category attribute of critical information are not to be displayed.

**Usage**

This command is useful when it is necessary to get real time output of events. Event output may be cached otherwise which may make it difficult to trouble shoot problems which do not allow the last cache of events to be output prior to system problems.

**Caution**: Issuing this command could negatively impact system performance depending on system loading, the log level, and/or the type of facility(ies) being logged.
Example
Set real time output for the point-to-point protocol facility and all facilities, respectively, to avoid logging of excessive information.

```
logging filter runtime facility ppp
logging filter runtime facility all level warning
```
logging monitor

Enables/disables the monitoring of a specified user.

Product
All

Privilege
Security Administrator, Administrator

Syntax

logging monitor { ipaddr ip_address | msid ms_id | username user_name }

no logging monitor { ipaddr ip_address | msid ms_id | username user_name }

```
no
Disables the monitoring of the user specified by the options given.
```

```
ipaddr ip_address
Specifies the IP address of the user for which the monitoring filter is to be set. ip_address must be an IP v4 address in dotted decimal notation.
```

```
msid ms_id
msid ms_id specifies the mobile subscriber ID for which the monitoring filter is to be set. ms_id must be from 7 to 16 digits.
This keyword/option can be used to specify the Mobile Subscriber ISDN (MSISDN) for GGSN calls which enables logging based on MSISDN.
```

```
username user_name
username user_name specifies a user for which the monitoring filter is to be set. user_name must refer to a previously configured user.
```

Usage
Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

⚠️ Caution: Issuing this command could negatively impact system performance depending on the number of subscribers for which monitoring is performed and/or the amount of data they’re passing.

Example
The following command enables the monitoring of user user1 and mobile subscriber ID 4441235555, respectively.

```
logging monitor username user1
logging monitor msid 4441235555
```
The following disables the monitoring of user `user1`.

```
no logging monitor username user1
```
mediation-device

This command is obsolete. Even though the CLI accepts the command no function is performed.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

mediation-device mode { tcs }

no mediation-device mode { tcs }

| tcs  
| N/A |

Usage
N/A

Example
N/A
network-overload-protection

This command configures an attach rate throttle mechanism to control the number of new connections (attaches or inter-SGSN RAUs), through the SGSN, on a per second basis.

Product  SGSN
Privilege Security Administrator, Administrator
Syntax

```
network-overload-protection sgsn-new-connections-per-second
action { drop | reject with cause { congestion | network failure } }
```

default network-overload-protection sgsn-new-connections-per-second

default
Using default in the command, disables this attach rate throttle feature.

```
#_new_connections
```
Define the number of new connections to be accepted per second.

```
#_new_connections: Must be an integer from 50 to 5000.
```

```
action
```
Specifies the action to be taken by the SGSN when the attach rate exceeds the configured limit on the number of attaches. Select one of the following actions:

- drop: Drop the new connection request.
- reject-with-cause: Reject the new connection request. Include one of the following as the cause in the reject message:
  - congestion
  - network failure

Usage
Use this command to configure the rate at which the SGSN must process new connection requests. The rate is the number of new connections to be accepted per second.
In some cases, the incoming new connection rate is higher than this configured rate. When this occurs, all of the new connection requests cannot be processed. This command can also be used to configure the action to be taken when the rate limit is exceeded. The new connection requests, which cannot be processed, can be either dropped or rejected with a specific reject cause.
Counters for this feature are available in the show gmm-sm statistics command display in the Network Overload Protection portion of the table.

Example
Configure the throttle rate or limit to 2500 attaches per second and to drop all requests if the limit is exceeded.
network-overload-protection sgsn-new-connections-per-second 2500 action drop
network-service-entity

This command creates a new instance of an SGSN network service entity for either the IP environment or the Frame Relay environment.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] network-service-entity ( ip-local | peer-nsei peer_nsei_number frame-relay )

no
Deletes the network service entity definition from the system configuration.

ip-local
Configures the local endpoint for NS/IP and enters the NSE-IP configuration mode. The prompt will change to [local]<hostname>(nse-ip-local)#

peer-nsei peer_nsei_number frame-relay
Configures a peer NSE and configures that peer with frame relay connectivity. This set of keywords also provides access to the NSE-FR configuration mode. The prompt will change to [local]<hostname>(nse-fr-peer-nsei<peer_nsei_number>)#

Usage
Use this command to access the configuration modes for either the IP or Frame Relay network service entities.

Example
Enter the NSE for a Frame Relay configuration instance identified as 4554:

network-service-entity peer-nsei 4554 frame-relay
network-service-entity ip

This command has been deprecated. See the replacement command network-service-entity.
ntp

Enters the network timing protocol configuration mode or disables the use of NTP on the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ntp
no ntp
```

**no**

Disables the use of NTP for clock synchronization. When omitted, the NTP client support is enabled on the chassis.

**Important:** If the use of NTP is disabled the system clock may drift over a period of time. This may require manual updates to the system clock to synchronize the clock with other network elements.

**Usage**

Used when it is necessary to configure NTP settings.

**Example**

The following command enters the NTP configuration mode:

```
ntp
```

The following disables the use of the network timing protocol for system clock synchronization.

```
no ntp
```
**operational-mode**

Configures the systems operational mode for general use or only as a home agent.

---

**Important:** This command is only required for code versions prior to 4.5.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
operational-mode {general | ggsn-only | ha-only}
```

- **general**
  
  Sets the system operational mode to general use allowing for FA, HA, PSDN, and/or GGSN services to be co-located.

- **ggsn-only**
  
  Configures the system to only allow Gateway GPRS Support Node (GGSN) services.

---

**Important:** Executing this keyword increases the maximum number of PDP contexts supported per Session Manager from 2000 to 4000.

- **ha-only**
  
  This command keyword has been deprecated and no longer performs any function.

---

**Usage**

Set the operational mode to segregating services across multiple systems.

---

**Caution:** In order for this command to function properly, this command must be executed prior to configuring services on the system.

---

**Example**

The following sets the operational mode to general and home agent, respectively.

```
operational-mode general
```
orbem

Enters the object request broker element manager configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

orbem

Usage
Set the configuration mode to allow modification of the ORB element manager configuration data.
pac-standby-priority

This command has been renamed to **card-standby-priority**. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.
port

The commands in this section set port parameters.
**port atm**

Identifies a physical port on a line card that supports ATM signaling and then enters the configuration mode for the specific interface-type. For the commands to configure the port interface, see the CLI chapter ATM Port Configuration Mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
port atm slot/port
```

- **atm**
  Indicates the port identified is an ATM interface port.

- **slot/port**
  To determine valid ATM slot and port numbers, use the Exec mode’s command `show port table`:
  - **slot**: Identifies the chassis slot holding the line card that supplies ATM ports. The slot ID number can be any valid integer between 17 and 48.
  - **port**: Identifies the physical port that is to be configured to support ATM signaling. The ID number can be any valid integer between 1 and 4.

**Usage**
Change the current configuration mode to Ethernet Port Configuration mode.

**Important**: This command is not supported on all platforms.

**Example**
The following enters the ATM port configuration mode for ATM port 1 on the card in slot 19:

```
port atm 19/1
```
port bits

Enters the BITS port configuration mode by identifying the BITS port on the active or standby SPIO.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
portbits slot/port
```

- `bits`:
  Identifies the BITS port.

- `slot/port`:
  - `slot`:
    Identifies the chassis slot holding the SPIO. The slot ID can be either 24 (active SPIO) or 25 (standby SPIO).
  - `port`:
    Identifies the BITS port on the SPIO. The port ID number must be 4.

**Usage**
Change the current configuration mode to BITS port configuration mode.

**Important**: This command is not supported on all platforms.

**Example**
The following enters the BITS port configuration mode for the active SPIO:
```
port bits 24/4
```
**port channelized**

Identifies a physical port on a channelized line card that supports Frame Relay signaling and creates a Frame Relay interface. As well, this command enters the configuration mode for the commands to configure the Frame Relay interface and the channelized port interface, see the CLI chapter Channelized Port Configuration Mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
portchannelized slot/port
```

**channelized**

Selects the channelized frame relay interface for the selected line card and port.

**slot/port**

To determine valid slots and port numbers, use the Exec mode’s command `show port table` to find the channelized line card.

- `slot`: Identifies the chassis slot holding the Channelized line card that supplies Frame Relay ports. The slot ID number can be any valid integer between 17 and 48.
- `port`: Identifies the physical port that is to be configured to support Frame Relay signaling. The ID number can only be 1.

**Usage**

Change the current configuration mode to Channelized Port configuration mode.

**Example**

The following enters the Channelized port configuration mode for port 1 on the card in slot 20:

```
port channelized 20/1
```
port ethernet

Enters the Ethernet Port Configuration mode for the identified port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
port ethernet slot/port
```

- **ethernet**
  - Indicates the port identified is an Ethernet interface port.

- **slot/port**
  - Specifies the port for which Ethernet Port Configuration mode is being entered. The slot and port must refer to an installed card and port.

Usage

Change the current configuration mode to Ethernet Port Configuration mode.

Example

The following enters the Ethernet Port Configuration mode for ethernet port 1 in slot 17:

```
port ethernet 17/1
```
port mac-address virtual-base-address

This command defines a block of 256 consecutive MAC addresses and enables virtual MAC addressing for Ethernet line card ports. Not available for the XT2 platform.

Product
All

Privilege
Security Administrator, Administrator

Syntax

port mac-address virtual-base-address MAC_Address

no port mac-address virtual-base-address

no
Disables virtual MAC addressing for Ethernet line card ports. The block of virtual MAC addresses is not saved.

MAC_Address
The beginning address of a block of 256 MAC addresses that are used for virtual MAC addressing.

Usage
Use this command to disregard the MAC addresses assigned and stored in the IDEEPROM on Ethernet Line Cards and assign MAC addresses for all ports on all Ethernet Line Cards from the specified block of virtual MAC addresses. This command does not affect the MAC addresses on SPIO cards.

There are 65536 MAC addresses (00:05:47:FF:00:00 - 00:05:47:FF:FF:FF) reserved for use by customers. This range allows for the creation of 256 address blocks each containing 256 MAC addresses (e.g. 00:05:47:FF:00:00, 00:05:47:FF:01:00, 00:05:47:FF:02:00, 00:05:47:FF:03:00, 00:05:47:FF:04:00, etc.).

Caution: This configuration requires the configuration of a valid block of unique MAC addresses that are not used anywhere else. Use of non-unique MAC addresses can degrade and impair the operation of your network.

Important: This command is not supported on all platforms.

Example
To enable virtual MAC addressing for Ethernet ports on all Ethernet line cards in the system using a block of MAC addresses starting at 00:05:47:FF:00:00, enter the following command:

port mac-address virtual-base-address 00:05:47:FF:00:00
**port rs232**

Enters the RS-232 Port Configuration mode for the RS-232 port on the specified SPIO card. Not available on the XT2 platform.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
port rs232 slot 3
```

**Usage**
Change the current configuration mode to RS-232 Port Configuration mode.

**Example**
The following command enters the RS-232 Port Configuration mode for the SPIO in slot 24;

```
port rs232 24 3
```
profile-id-qci-mapping

Creates a QCI - RAN ID mapping table or specifies an existing table and enters the QCI - RAN ID mapping configuration mode for the system.

Product
HSGW

Privilege
Administrator

Syntax

[ no] profile-id-qci-mapping name [ -noconfirm ]

- no
Removes the specified mapping table from the system

- name
Creates a new or enters an existing mapping table configuration. name must be from 1 to 63 alpha and/or numeric characters.

- -noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Enters the QCI - RAN ID mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.
Entering this command results in the following prompt:
[context_name]hostname(config-hsgw-association-table)#
QCI Mapping Configuration Mode commands are defined in the QCI Mapping Configuration Mode Commands chapter.
Use this command when configuring the following eHRPD component: HSGW.

Important: This command creates a mapping table available to any HSGW context configured on the system.

Example
The following command enters the existing QCI mapping configuration mode (or creates it if it doesn’t already exist) for a mapping table named qci_table1:

    profile-id-qci-mapping qci_table1

The following command will remove qci_table1 from the system:

    no profile-id-qci-mapping qci_table1
**ps-network**

This command creates/removes an HNB-PS network configuration instance for Femto UMTS access over Iu-PS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and PS networks elements; i.e. SGSN. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

**Product**

HNB-GW

**Privilege**

Administrator

**Syntax**

```
[no] ps-network ps_instance [-noconfirm]
no ps-network ps_instance
```

**no**

Removes the specified HNB-PS network instance from the system.

⚠️ **Caution:** Removing the HNB-PS network instance is a disruptive operation and it will affect all UEs accessing SGSN(s) in specific PS core network through the HNB-GW service.

⚠️ **WARNING:** If any HNB-PS Network instance is removed from system all parameters configured in that mode will be deleted and Iu-PS/Iu-Flex interface will be disabled.

---

**ps_instance**

Specifies the name of the Packet Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN in HNB RN-PLMN configuration mode. If `ps_instance` does not refer to an existing HNB-PS instance, the new HNB-PS network instance is created.

`ps_instance` must be from 1 to 63 alpha and/or numeric characters.

---

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.

---

**Usage**

Use this command to enter the HNB-PS Network Configuration mode for an existing PS network instance or for a newly defined HNB-PS network instance. This command is also used to remove an existing HNB-PS network instance.

This configuration enables the Iu-PS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.

A maximum of 8 HNB-PS networks instance can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

⚠️ **Caution:** This is a critical configuration. The HNBs can not access SGSNs in PS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to PS core network.
Entering this command results in the following prompt:

```
[context_name]hostnam{config-ps-network}#
```

The various parameters available for configuration of an HNB-PS network instance are defined in the HNB-PS Network Configuration Mode Commands chapter of Command Line Interface Reference.

---

**Example**

The following command enters the existing HNB-PS Network configuration mode (or creates it if it doesn’t already exist) for the instance named `hnb-ps1`:

```
ps-network hnb-ps1
```

The following command will remove HNB-PS network instance `hnb-ps1` from the system without any prompt to user:

```
no ps-network hnb-ps1
```
qci-qos-mapping

Global QCI-QoS mapping tables are used to map QCI values to appropriate QoS parameters.

Product
HSGW, P-GW, S-GW

Privilege
Administrator

Syntax

qci-qos-mapping name [ -noconfirm ]

no
Removes the specified mapping configuration from the system

name
Creates a new or enters an existing mapping configuration. name must be from 1 to 63 alpha and/or numeric characters.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Enter the QCI-QoS mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.

Entering this command results in the following prompt:

[context_name]hostname(config-qci-qos-mapping)#

QCI - QoS Mapping Configuration Mode commands are defined in the QCI - QoS Mapping Configuration Mode Commands chapter.

Use this command when configuring the following eHRPD component: HSGW, P-GW, S-GW.

Important: This command creates a mapping configuration available to any HSGW, P-GW, S-GW context configured on the system.

Example

The following command enters the existing QCI - QoS mapping configuration mode (or creates it if it doesn’t already exist) for a mapping configuration named qci-qos3:

qci-qos-mapping qci-qos3
qos npu inter-subscriber traffic bandwidth

Configures NPU QoS bandwidth allocations for the system.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
quos npu inter-subscriber traffic bandwidth
  gold percent
gold percent
```

```
silver percent
default: 20%
specifies the maximum percentage of bandwidth to be allocated to the silver queue priority.
percent can be configured to any integer value from 0 to 100.
```

```
bronze percent
default: 30%
specifies the maximum percentage of bandwidth to be allocated to the bronze queue priority.
percent can be configured to any integer value from 0 to 100.
```

```
best-effort percent
default: 40%
specifies the maximum percentage of bandwidth to be allocated to the best-effort queue priority.
percent can be configured to any integer value from 0 to 100.
```

**Usage**
The bandwidth of a subscriber queue is maintained by rate limiting functions which implement packet-rate limiting at the first level and bit-rate limiting at the next level.
The packet-rate limit of a queue is defined by the number of packets-per-second (PPS) permitted for queuing.
Before queuing a packet on a subscriber queue, the NPU ensures that the packet falls within the limit. If the packet to be queued exceeds the packet rate limit, it is dropped.
Each subscriber queue is configured with a bit rate limit, measured in megabits-per-second (Mbps), referred to as CP-BPS (bit-per-second to CP). The CP-BPS is available as the total bandwidth for the subscriber traffic.
that a CP can sustain. Each subscriber queue receives an allocation of a certain percentage of the CP-BPS. The following maximum CP-BPS values are supported:
- Lead CP (CP0) = 128 Mbps
- Remaining CPs (CP1, CP2, CP3) = 256 Mbps

For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

**Important:** This functionality is not supported for use with the PDSN at this time.

**Example**
The following command configures bandwidth allocations of 20, 30, 40, and 50% for the gold, silver, bronze, and best-effort queues respectively:

```
qos npu inter-subscriber traffic bandwidth gold 20 silver 30 bronze 40 best-effort 50
```

Upon executing this command, the priority queues will have the following PSC/PSC2 CP bandwidth allocations based on the maximum CP bandwidth specifications:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Lead CP (CP 0) Bandwidth (Mbps)</th>
<th>CP 1 through CP 3 Bandwidth (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>25.6</td>
<td>51.2</td>
</tr>
<tr>
<td>Silver</td>
<td>38.4</td>
<td>76.8</td>
</tr>
<tr>
<td>Bronze</td>
<td>51.2</td>
<td>102.4</td>
</tr>
<tr>
<td>Best-effort</td>
<td>64</td>
<td>128</td>
</tr>
</tbody>
</table>
qos npu inter-subscriber traffic bandwidth-sharing

Configures NPU QoS bandwidth sharing properties for the system.

**Product**
PDSN, GGSN

**Privilege**
Administrator

**Syntax**

```
qos npu inter-subscriber traffic bandwidth-sharing { { enable | disable } { all | slot slot_num | cpu cpu_num } }
```

- **enable**
  Enables bandwidth sharing for the specified criteria.

- **disable**
  Disables bandwidth sharing for the specified criteria.

- **all**
  Specifies that the bandwidth action is to be applied to all PSC/PSC2s and every CPU on each PSC/PSC2.

- **slot slot_num**
  Specifies that the bandwidth action is to be applied to a PSC/PSC2 in a specific chassis slot number. `slot_num` is an integer from 1 to 48 that represents the slot in which a PSC/PSC2 is installed. These cards can be installed in slots 1 through 8, and/or 10 through 16.

- **cpu cpu_num**
  Specifies a specific PSC/PSC2 CP for which to perform the bandwidth action. `cpu_num` is an integer value from 0 to 3. 0 represents the lead CP.

**Usage**

The available bandwidth of a subscriber queue can be shared equally among the other subscriber queues. Any unutilized bandwidth of a queue can be shared with the other queues equally. For example, if only one DSCP is configured and it is mapped to best-effort, that DSCP would get the bandwidth allocated to the best-effort in addition to the rest of the bandwidth allocated to the gold, silver, and bronze. By default, the system enables sharing for all PSCs or PSC2s and their CPs. For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

**Important:** This functionality is not supported for use with the PDSN at this time.

**Example**

```
```
The following command disables bandwidth sharing for the fourth CP (CP 3) on a PSC/PSC2 installed in chassis slot 4:

```
qos npu inter-subscriber traffic bandwidth-sharing disable slot 4 cpu 3
```
qos npu inter-subscriber traffic priority

Configures the DSCP-to-Priority assignments for the system.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

qos npu inter-subscriber trafficpriority { best-effort | bronze | gold | silver |
assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | be | ef | dscp_num } }

no qos npu inter-subscriber trafficpriority [ assigned-to dscp { af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } ]

best-effort
Specifies the best-effort queue priority.

bronze
Specifies the bronze queue priority.

gold
Specifies the gold queue priority.

silver
Specifies the silver queue priority.

afXX
Assigns the Assured Forwarding $XX$ PHB DSCP. Each Assured Forwarding PHB has a corresponding DSCP value as follows:
- af11 through af13: DSCP values 5 through 7 respectively
- af21 through af23: DSCP values 9 through 11 respectively
- af31 through af33: DSCP values 13 through 15 respectively
- af41 through af43: DSCP values 17 through 19 respectively

be
Assigns the Best Effort forwarding PHB which has a corresponding DSCP value of 0.

ef
Assigns the Expedited Forwarding PHB which has a corresponding DSCP value of 23.
Specifies a specific DSCP value. The value must be expressed as an integer value from 0 through 31.

Usage

The differentiated services (DS) field of a packet contains six bits (0-5) that represent the differentiated service code point (DSCP) value. Five of the bits (1-5) represent the DSCP. Therefore, up to 32 (2^5) DSCPs can be assigned to the various priorities. By default, they're all assigned to the lowest priority (best-effort). For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

Important: This functionality is not supported for use with the PDSN at this time.

Example

The following command maps the ef DSCP to the gold priority queue:

```
qos npu inter-subscriber traffic priority gold assigned-to dscp ef
```
**ran-peer-map**

Creates a RAN Peer Map and enters the RAN Peer Map Configuration Mode.

**Product**
ASN GW, PHS

**Privilege**
Administrator

**Syntax**

```bash
[ no ] ran-peer-map name [ -noconfirm ]
```

---

**no**
Removes the RAN Peer Map from the system.

---

**name**
Specifies the name of the RAN Peer Map. *name* must be from 1 to 31 alpha and/or numeric characters.

---

**Usage**

Use this command to create a new RAN Peer Map or edit an existing one. RAN peer maps reconcile base station MAC addresses received in R6 protocol messages to the base station’s IP address. Entering this command results in the following prompt:

```
[context_name]hostname(config-ran-peer-map)#
```

RAN Peer Map Configuration Mode commands are defined in the ASN RAN Peer Map Configuration Mode Commands chapter in this guide.

---

**Example**
The following command creates a RAN peer map named *ran12*:

```bash
ran-peer-map ran12
```
require active-charging

This command enables/disables Active Charging Service (ACS) with or without Category-based Content Filtering application.

Product
ACS, CF

Privilege
Security Administrator, Administrator

Syntax
require active-charging [ isolated-mode ] [ content-filtering category [ static-and-dynamic ] ] [ optimized-mode ]

no require active-charging

---

**isolated-mode**

Enables ACS, and separates ACS-related resources from other sub-system resource sharing.

**Important:** In Release 8.1 and later, this keyword is not supported.

**optimized-mode**

Enables ACS in Optimized mode, wherein ACS functionality is managed by SessMgrs.

**Important:** In Release 8.0 and earlier and in Release 9.0 and later, this keyword is not supported.

**Important:** In Release 8.1, ACS must be configured in the Optimized mode.

**Important:** In Release 8.1, if the active-charging mode is changed from the default (Non-optimized) mode to the Optimized mode, or vice-versa, the system must be rebooted for the change to take effect.

**Important:** In Release 8.3, this keyword is obsolete. With or without this keyword ACS is always enabled in Optimized mode.

Use the `require active-charging` command to enable ACS in the non-optimized mode. Wherein, ACSMgrs will spawn to support ACS.

Use the `require active-charging optimized-mode` command to enable ACS in the Optimized mode. Wherein, ACS is enabled as part of SessMgr.
content-filtering category [ static-and-dynamic ]

Enables the Category-based Content Filtering application with Active Charging support and creates the necessary Static Rating Database (SRDB) tasks to utilize the internal database of static/dynamic URLs. For Dynamic Content Filtering support, the `static-and-dynamic` keyword must be configured to specify that the Dynamic Rater Package (model and feature files) must be distributed to rating modules on startup, recovery, etc. If not configured, by default, the static-only mode is enabled.

**Usage**

Use this command to enable/disable ACS with or without Category-based Content Filtering application on a system.

In Release 8.0 and 8.1, this command must be configured before configuring any services. This is to ensure that the resource subsystem can appropriately reserve adequate memory for ACS Manager (ACSMgr) tasks. If this command is configured after all the Session Manager (SessMgr) tasks are already active, the ACSMgr tasks will not be started even if additional cards are added to the chassis—instead, the chassis must be rebooted.

**Example**

In Release 8.0, the following command enables resource subsystem to configure ACS in isolated mode:

```
require active-charging isolated-mode
```

In Release 8.1, the following command enables ACS in Optimized mode:

```
require active-charging optimized-mode
```

In Release 8.3, the following command enables ACS in Optimized mode:

```
require active-charging
```
**require demux card**

This command enables/disables the demux capabilities.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[default | no ] require demux card
```

- **default**
  Disables the demux capabilities on the card.

- **no**
  Disables the demux capabilities on the card.

**Usage**

Use this command configure the system to allow session recovery task placement scheme when session recovery is off.

**Important:** This command is not supported on all platforms.

**Example**
The following command enables demux capabilities:

```
require demux card
```
require detailed-rohc-stats

Enables or disables context-specific Robust Header Compression (RoHC) statistics.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
[ no ] require detailed-rohc-stats
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables require detailed-rohc-stats. This is the default condition.</td>
</tr>
</tbody>
</table>

**Usage**
Enables context-specific statistics for RoHC calls.

**Example**
Enter the following command to enable context specific stats for RoHC calls:

```
require detailed-rohc-stats
```
require diameter-proxy

This command enables/disables Diameter Proxy mode.
Default: no require diameter-proxy

Product
All

Privilege
Security Administrator, Administrator

Syntax

require diameter-proxy { multiple | single }  
no require diameter-proxy

Usage
When the Diameter Proxy mode is enabled, each proxy process is a Diameter host, instead of requiring every Diameter application user (i.e., every ACSMgr and/or every SessMgr, depending on the application) to be a host.

Example
To configure a Diameter proxy for each active PSC/PSC2, enter the following command:

require diameter-proxy multiple

To configure a single Diameter proxy for the entire chassis, enter the following command:

require diameter-proxy single
require session recovery

Enables session recovery when hardware or software fault occurs within system.

Product
PDSN, GGSN, SGSN, HA, LNS, ASN GW, PDIF, MME

Privilege
Security Administrator, Administrator

Syntax
require session recovery

no require session recovery

Usage
When this feature is enabled, the system attempts to recover any home agent-based Mobile IP sessions that would normally be lost due to a hardware or software fault within the system. This functionality is available for the following call types:
- ASN GW services supporting simple IP, Mobile IP, and Proxy Mobile IP
- PDSN services supporting simple IP, Mobile IP, and Proxy Mobile IP
- HA services supporting Mobile IP and/or Proxy Mobile IP session types with or without per-user Layer 3 tunnels
- GGSN services for IPv4 and PPP PDP contexts
- SGSN services for all attached and/or activated subscribers
- LNS session types
- PDIF services supporting Simple-IP, Mobile-IP, and Proxy Mobile-P
- MME services

The default setting for this command is disabled. The no option of this command disables this feature. It is important to note that this command only works when the Session Recovery feature is enabled through a valid Session and Feature Use License Key.

Important: Upon entering this command, the system must be restarted before the command takes effect. Remember to save the configuration file before issuing the reload command.
reveal disabled commands

Enables the input of commands for features that do not have license keys installed. The output of the command `show cli` indicates when this is enabled. This command effects all future CLI sessions. This is disabled by default.

Product
All

Privilege
Security Administrator, Administrator

Syntax

reveal disabled commands

no reveal disabled commands

Usage
When this is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command. When this is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

Example
Set the CLI to accept disabled commands and display the required feature for all future CLI sessions with the following command:

`reveal disabled commands`

Set the CLI to reject disabled commands and return an error message for all future CLI sessions:

`no reveal disabled commands`
rohc-profile

This command allows you to create an RoHC (Robust Header Compression) profile and enter the RoHC Profile Configuration Mode. This mode is used to configure RoHC Compressor and Decompressor parameters. RoHC profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured.

Product
HSGW, PDSN

Privilege
Security Administrator, Administrator

Syntax

rohc-profile profile-name name [ -noconfirm ] [common-options | compression-options| decompression-options]

no rohc-profile profile-name name

---

common-options
Configures common parameters for compressor and decompressor.

compression-options
Configures ROHC compression options.

decompression-options
Configures ROHC decompression options.

no
Remove the specified RoHC profile.

name
The name of the RoHC profile to create or remove. name must be an alphanumeric string of from 1 through 63 characters in length.

-noconfirm
Do not prompt for additional verification when executing this command.

Usage
Use this command to enter the RoHC Profile Configuration mode.
Entering this command results in the following prompt:

[context_name]host(config-rohcprofile<profile_name>)#

RoHC Profile Configuration Mode commands are defined in the RoHC Profile Configuration Mode Commands chapter.

Example
Enter the following command to create an RoHC profile named `HomeUsers` and enter the RoHC Configuration mode without prompting for verification:

```
rohc-profile profile-name HomeUsers
```

The following command removes the RoHC profile named `HomeUsers`:  

```
no rohc-profile profile-name HomeUsers
```
sccp-network

This command creates or removes a Signaling Connection Control Part (SCCP) network instance which is used to define the SS7 end-to-end routing in a UMTS network. As well, this command enters the SCCP network configuration mode. The SGSN supports up to 12 SCCP network instances at one time.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
sccp-network sccp_net_id [-noconfirm]

no sccp-network sccp_net_id
```

- **no**
  Remove the SCCP network configuration with the specified index number from the system configuration.

- **sccp_net_id**
  This number identifies a specific SCCP network configuration.
  *sccp_net_id:* must be an integer from 1 through 12.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create or modify an SCCP network and enter the SCCP network configuration mode. The SCCP network is not a standard SS7 or UMTS concept - this concept is specific to this platform. For details about the commands and parameters needed to create and edit the SCCP Network configuration, check the *SCCP Network Configuration Mode* chapter.

Example

The following command creates an SCCP network with the index number of 1:

```
sccp-network 1
```

The following command creates an SCCP network with the index number of 2 to associate with HNB-GW service for HNB access network users without any prompt:

```
sccp-network 2 -noconfirm
```
session trace

This command configures the type of network elements, file transfer protocol, and Trace collection entity mode to be used for the transportation of trace files collected for the subscriber session tracing on the EPC network element(s) along with network connection parameters and timers.

Product
MME, P-GW, S-GW

Privilege
Administrator

Syntax

```
session trace [ collection-timer sec ] [ network-element { all | mme | pgw | sgw } ] [ retry-timer sec ] [ tce-mode { none | push transport { ftp | sftp } path string username name { encrypted password enc_pw | password password } ] ]
```

```
no session trace [network-element {all | mme | pgw | sgw}]
```

no
Removes the entire session trace configuration from the system or a specific network element trace configuration.

```collection-timer sec```
Specifies the amount of time, in seconds, to wait from initial activation/data collection before data is reported to the Trace Collection Entity (TCE). `sec` must be an integer value from 0 to 255.

```network-element {all | mme | pgw | sgw}```
Identifies the type of service to the session trace application in order to determine the applicable interfaces.
- **all**: Specifies that all network elements and their associated interfaces are to be made available to the session trace application.
- **mme**: Specifies that the MME network element and its associated interfaces is to be made available to the session trace application.
- **pgw**: Specifies that the P-GW network element and its associated interfaces is to be made available to the session trace application.
- **sgw**: Specifies that the P-GW network element and its associated interfaces is to be made available to the session trace application.

```retry-timer sec```
Specifies the amount of time, in seconds, to wait before retrying a file transfer after a failure. `sec` must be an integer value from 0 to 255.

```tce-mode none```
Specifies that session trace files are to be stored locally and must be pulled by the TCE.
Global Configuration Mode Commands

**session trace**

```plaintext
tce-mode push transport \{ ftp | sftp \} path string username name \{ encrypted password enc_pw | password password \}
```

Specifies that session trace files are to be pushed to the Trace Collection Entity (TCE).
- `{ ftp | sftp }`: Specifies that FTP or Secure FTP is used to push session trace files to the TCE.
- `path string`: Specifies the directory path on the TCE where files will be placed.
- `username name`: Specifies the username to be used when pushing files to the TCE.
- `encrypted password enc_pw`: Specifies the encrypted password to be used when pushing files to the TCE.
- `password password`: Specifies the password to be used when pushing files to the TCE.

**Usage**

Use this command to configure the file transfer methods and modes for subscriber session trace functionality and to how and where session trace files are sent after collection.
This configuration contains collection timer, EPC network element, type of file transfer, and user credentials setting to send the collected trace files to the TCE.

**Example**

The following command configures the collection time for session traces to 30 seconds, identifies the network element as all elements (MME, S-GW, and P-GW), sets the retry timer to 5 seconds, and pushes session trace files to a TCE via SFTP into a directory named `/trace/sgw` using a username `admin` and a password of `pw123`:

```
session trace collection-timer 30 network-element all retry-timer 5 tce-mode push transport sftp path /trace/sgw username admin password pw123
```

The following command configures the collection time for session traces to 30 seconds, identifies the network element as an MME, sets the retry timer to 5 seconds, and pushes session trace files to a TCE via SFTP into a directory named `/trace/mme` using a username `admin` and a password of `pw123`:

```
session trace collection-timer 30 network-element mme retry-timer 5 tce-mode push transport sftp path /trace/mme username admin password pw123
```
**sgsn-operator-policy**

This command creates an SGSN Operator Policy and enters the SGSN operator policy configuration mode. Commands for configuration of the policies are available in the SGSN Operator Policy Configuration Mode chapter elsewhere in this Command Line Interface Reference.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

sgsn-operator-policy { default | name name } [ -noconfirm ]

no sgsn-operator-policy { default | name name }

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

- **no**
  Remove the specified SGSN operator policy from the system configuration.

- **default**
  default, in this case, is the name of a specific operator policy. This default policy is used when no other defined operator policy matches the incoming IMSI.

**Important:** We recommend that you configure this default operator policy so that it is available to handle IMSIs that are not matched with other defined policies.

**Usage**

Use this command to create an SGSN operator policy and to enter the SGSN operator policy configuration mode to define or modify policies. The SGSN Operator Policy specifies rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs. The system supports up to 1000 operator policies, including the default operator policy.

**Important:** Once the instance of an operator policy is defined, to use the policy it is necessary to go into the SGSN Operator Policy Configuration Mode to define the IMSI range with the MCC command - this requirement does not hold if you are using a default operator policy.

**Example**
The following command accesses the default SGSN operator policy and enters the SGSN operator policy configuration mode to view or modify the specified policy:

```bash
sgsn-operator-policy default
```
snmp

The commands in this section set SNMP parameters.
snmp authentication-failure-trap

Enables/disables the SNMP traps for authentication failures.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
no snmp authentication-failure-trap
```

**Usage**

Disables authentication failure traps if they are not of interest. At this time the option may be changed to support trouble shooting.

The chassis is shipped from the factory with the SNMP authentication failure traps disabled.


### snmp community

Configures the SNMP v1 and v2 community strings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```markdown
snmp community string [ context ctx_name ] [ view view_name ] [ read-only | read-write ]
```

```markdown
no snmp community string
```

---

**no**

The specified community string is removed from the configuration.

---

**string**

Specifies a community string whose options are to be modified. `string` must be a from 1 to 31 alpha and/or numeric characters.

---

**context ctx_name**

Default: community string applies to all contexts.

Specifies a the context to which the community string shall be applied. `ctx_name` must be from 1 to 1023 alpha and/or numeric characters.

---

**view view_name**

Default: community string applies to all views.

Specifies the view to which the community string shall be applied. `view_name` must from 1 to 1023 alpha and/or numeric characters.

---

**read-only | read-write**

Default: read-only

Specifies if access rights for the community string.

- **read-only**: the configuration may only be viewed.
- **read-write**: the configuration may be viewed and edited.

---

**Usage**

The community strings define the privileges of SNMP users. It may be desirable to give read-only access to front line operators.

---

**Example**
snmp community sampleString
snmp community sampleString context sampleContext
snmp community sampleString context sampleContext view sampleView
snmp community sampleString view sampleView read-write
no snmp community sampleString
### snmp engine-id

Configures the SNMP engine to use for SNMP requests when SNMPv3 agents are utilized.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
snmp engine-id local id
```

*id*

Specifies the SNMPv3 engine to employ. *id* must be from 1 to 31 alpha and/or numeric characters.

**Usage**

When SNMPv3 is used for SNMP access to the chassis the engine ID can be used to quickly change which schema is used for SNMP access.

**Important:** The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

**Example**

```
snmp engine-id local id
```
snmp heartbeat

Enables the sending of periodic “heartbeat” notifications (traps).

Product
All

Privilege
Administrator

Syntax

```
snmp heartbeat { interval [ minutes ] | second-interval [ seconds ] }

deafult snmp heartbeat

no snmp heartbeat
```

- **default**
  Returns the command to its default setting of disabled.

- **no**
  Disables the feature.

- **interval [ minutes ]**
  Default: 60
  Specifies the interval time, in minutes, between notifications. minutes must be an integer value between 1 and 1440.

- **second-interval [ seconds ]**
  Default: 30
  Specifies the secondary interval time, in seconds, between notifications. seconds must be an integer value between 10 and 50.

Usage

Use this command to enable the sending of a heartbeat notification periodically to confirm a system is up and communicating.

Example

The following command sets the snmp heartbeat notification interval to 2 hours, 15 minutes and 30 seconds:

```
snmp heartbeat interval 135 second-interval 30
```
**snmp history heartbeat**

Enables the recording of heartbeat notifications in SNMP history.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
[ default | no ] snmp history heartbeat
```

- **default**
  Returns the command to the default setting of enabled.

- **no**
  Disables the history recording feature.

**Usage**

Use this command to enable the recording of SNMP heartbeat notifications in SNMP history files.
snmp notif-threshold

Configures the number of SNMP notification that need to be generated for a given event before it is propagated to the SNMP users.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
snmp notif-threshold count [ low low_count ] [ period seconds ]
```

```
no snmp notif-threshold
```

**no**

Removes all SNMP notification thresholds. All notifications will be broadcast to SNMP users.

**count**

Default: 100
Specifies the number of notifications that must be generated before the next notification is broadcast to SNMP users. `count` must be a value in the range from 1 to 10000.

**low low_count**

Default: 20
Specifies the number of notifications within the monitoring period before which any subsequent notification for each specific event. `low_count` must be a value in the range from 1 through 10000.

**period seconds**

Default: 300
Specifies the number of seconds of the monitoring window size used to determine when any subsequent notification may be broadcast to users. `seconds` must be a value in the range from 10 through 3600.

Usage

Set the notification threshold to avoid a flood of events which may be the result of a single failure or maintenance activity.

Example

```
snmp notif-threshold 100
```

```
snmp notif-threshold 100 period 30
```
**snmp server**

Enables the SNMP server as well the configuration of the SNMP server port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
snmp server [ port number ]
```

```
no snmp server
```

- **no**
  Restores the default SNMP port assignment.

- **port number**
  Default: 161
  Specifies the port number to use for SNMP communications. *number* must be a value in the range from 1 to 65535.

**Usage**
Set the SNMP port for communications when SNMP is enabled.

**Important:** This will result in restarting the SNMP agent when the `no` keyword is omitted. SNMP queries as well as notifications/traps will be blocked until the agent has restarted.

**Example**

```
snmp server port 100

no snmp server
```
**snmp target**

Configures remote receivers of SNMP notifications.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
snmp targetname ip_address [ portnumber ] [ non-default ] [ security-namestring ] [ version { 1 | 2c | 3 | view } [security-level { noauth | { auth | priv-auth } privacy [encrypted] des privpassword } authentication [encrypted] { md5 | sha } authpassword } ] [ informs | traps ]
```

```plaintext
no snmp targetname
```

**no**

Removes the specified target as a receiver of unsolicited SNMP messages.

```plaintext
authentication { md5 | sha } authpassword
```

Reads the authentication type and password if the security level of the SNMP messages is set to `auth` or `priv-auth`. Authentication types are:
- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **sha**: Specifies that the hash protocol is Secure Hash Algorithm.

```plaintext
security-level { noauth | { auth | priv-auth } privacy [encrypted] des privpassword }
```

Sets the security level of the SNMPv3 messages, as follows:
- **noauth**: No authentication and encryption is used.
- **auth**: Only authentication will be used.
- **priv-auth**: Both authentication and encryption will be used.
- **privacy des privpassword**: Reads the privacy type and password.

```plaintext
name
```

Specifies a logical name to use to refer to the remote receiver. `name` must be from 1 to 31 alpha and/or numeric characters.

```plaintext
ip_address
```

Specifies the IP address of the receiver. `ip_address` must be specified using the standard IPv4 dotted decimal notation.

```plaintext
non-default
```

Specifies that this destination is only used for SNMP traps which have been specifically identified.
**port number**
Default: 162
Specifies the port which is to be used in communicating with the remote receivers. `number` must be a value in the range from 0 through 65535.

**security-name string**
Default: no community string included
Specifies the community string to use in the unsolicited messages. `string` must be from 1 to 31 alpha and/or numeric characters.

**version { 1 | 2c | 3 | view }**
Default: 1
Specifies the SNMP version the target supports and consequently the version of the SNMP protocol to use for communications.

---

**Important:** The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must configure this command to use version 1 or version 2c.

**informs | traps**
Default: traps
Specifies the type of SNMP event to use to send notifications to SNMP targets. `traps` are unacknowledged (fire and forget) whereas `informs` require a response from the SNMP target.
If the notification type is set to `informs`, the notification is resent if no response is received within 5 seconds. The notification is resent at most two times.

**Usage**
The target manages the list of remote receivers to which unsolicited messages are sent, e.g., this is necessary if a new monitoring system is added to a network or removed.

**Example**

```bash
snmp target sampleReceiver 1.2.3.4 security-name sampleComm
snmp target sampleReceiver 1.2.5.6 port 100
snmp target sampleReceiver 1.2.7.8 version 2c traps
no snmp target sampleReceiver
```
snmp trap

This command enables/disables generation of specific or all SNMP traps.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
snmp trap { enable | suppress } [trap_name1 trap_name2 ... trap_nameN| all ]
```

- **enable**
  Enables or allows the generation of one or more SNMP traps by the system.

- **suppress**
  Disables the generation of one or more SNMP traps by the system.

- **trap_name1 trap_name2 ... trap_nameN**
  The name of the specific SNMP trap to enable or disable. Multiple traps can be listed for a single instance of this command.

**Important:** The system disregards character case when entering trap names.

- **all**
  Default: Enable All
  Specifies that all SNMP traps will be affected by the specified operation (enable or suppress).

**Usage**

SNMP traps are used by the system to indicate that certain events have occurred. A complete listing of the traps supported by the system and their descriptions can be found in the SNMP MIB Reference. Additionally, a trap listing can be viewed using the following command:

```
snmp trap { enable | suppress }?
```

By default, the system enables the generation of all traps. However, individual traps can be disabled allowing only traps of a certain type or alarm level to be generated. This command can be used to disable un-desired traps and/or re-enable previously suppressed traps.

**Example**

The following command suppresses the LogMessage trap:

```
snmp trap suppress logmessage
```

The following command suppresses the `CLISessEnd` and `CLISessStart`: 

---
snmp trap suppress clisessend clisessstart
snmp trap-timestamps

Adds an additional system-time varbind to generated traps.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] snmp trap-timestamps

no

Disables the adding of timestamps to generated traps.

Usage

The timestamp added to the generated trap reflects the current system time. The timestamp is proprietary. This functionality is disabled by default.

Important: If the Web Element Manager application is used as your alarm server, the application relies on the timestamp provided by enabling this command to identify duplicate traps. As a result, it is recommended that this parameter be enabled for this case.

Example

The following command enables the inclusion of a timestamp with each generated trap:

snmp trap-timestamps
snmp user

Configures an SNMPv3 user for SNMP access.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
  snmpuser user_name [ [ encrypted ] password password | engine id | group grp_name | security-model model auth [ [ encrypted ] password password ] ]
  no snmp user user_name
```

- **no**
  Removes the specified user from the list of valid SNMPv3 users.

- **user_name**
  Specifies the user which is to use SNMPv3 interfaces to the system. `user_name` must be from 1 to 31 alpha and/or numeric characters.

- **engine id**
  The SNMP engine ID. `id` must be a string of alpha and/or numeric characters from 1 to 31 characters in length.

- **group grp_name**
  Default: undefined (not a member of any group)
  Specifies the user SNMPv3 group the into which user will be added. `grp_name` must be from 1 to 1023 alpha and/or numeric characters.

- **security-model model auth**
  Default: USM
  Specifies the security model used to authenticate the user. `model` must be configured to the following:
  - `usm`: User Security Model

- **[ encrypted ] password password**
  Default: undefined
  Specifies the password for authenticating the user when the security model is set to USM.
  The `encrypted` keyword indicates the password will be received in an encrypted form. `password` must be from 8 to 31 alpha and/or numeric characters.
  The `encrypted` keyword is intended only for use by the chassis while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
Usage
Add and remove SNMPv3 users as operations staff or automated systems are updated. The security model will be user dependant based upon the support the users system provides.

Important: The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

Example

```
snmp user user1

snmp user user1 security-model 2c auth

snmp user user1 group sampleGroup security-model usm auth

no snmp user user1
```
ss7-routing-domain

This command creates an SS7 routing domain instance and enters the SS7 routing domain configuration mode.

**Product**
SGSN, HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ss7-routing-domain rd_id variant v_type [-noconfirm]

no ss7-routing-domain rd_id
```

- **no**
  Removes the specified SS7 routing domain from the system configuration.

- **rd_id**
  This number identifies a specific SS7 routing domain. Once it has been created, it can be accessed for further configuration and modification by entering the `rd_id` without entering the variant. `rd_id` must be an integer from 1 to 12.

- **variant v_type**
  Identifies the national standard to be used for call setup, routing and control, signaling. Select one of the following:
  - `ansi`: American National Standards Institute (U.S.A.)
  - `bici`: Broadband Intercarrier Interface standard
  - `china`: Chinese standard
  - `itu`: International Telecommunication Union (ITU-T) Telecommunication Standardization Sector
  - `ntt`: Japanese standard
  - `ttc`: Japanese standard

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create an SS7 routing domain configuration instance or to enter the SS7 routing domain configuration mode to edit the configuration.

A routing domain groups configuration items to facilitate the management of the SS7 connection resources for an SGSN service. An Access Gateway supports up to 12 configured SS7 routing domains at one time. After entering this command, the prompt appears as:

```
[context_name]<hostname> (config-ss7-routing-domain-routing_domain_id) #
```

For details about the commands and parameters used to define or edit an SS7 routing domain, refer SS7 Routing Domain Configuration Mode chapter.
Example
The following creates an SS7 routing domain with an index of 1 and the variant selection of Broadcast Intercarrier Interface (bici):

```
ss7-routing-domain 1 variant bici
```

The following command creates an SS7 routing domain instance with an index of 2 and the variant selection of Broadcast Intercarrier Interface (bici) to be associated with HNB RN-PLMN in an HNB access network:

```
ss7-routing-domain 2 variant bici
```
suspend local-user

Suspends a local-user administrative account.

Product
All

Privilege
Administrator

Syntax

```
suspend local-user name

no suspend local-user name
```

- **no**
  Removes the suspended status for the specified local-user account.

- **name**
  The name of the local-user account. It can be from 3 to 16 alpha and/or numeric characters and is case sensitive.

Usage
This command allows a security administrator to suspend local-user administrative accounts. A “suspended” user can not login to the system. The user’s account information (passwords, password history, etc.), however, is preserved.

Example
The following command suspends a local-user account called Inspector1:

```
suspend local-user Inspector1
```

The following command removes the suspension from a local-user account called Admin300:

```
no suspend local-user Admin300
```
system

Configures system information which is accessible via SNMP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
system { carrier-id mcc_id mnc_id | contact who | hostname host_name | location text }
```

default system { contact | location }

default
This keyword removes the configured system contact and system location on system.

carrier-id mcc mcc_id mnc mnc_id

Important: This carrier ID is not used by the GGSN

This keyword specifies a carrier-id that is a unique identifier for the carrier that has installed the system. When the carrier ID values are set, the carrier-id and gmt_offset attributes are included in access-request and accounting packets when using the following RADIUS dictionaries:

- 3gpp2
- 3gpp2-835
- starent
- starent-835
- starent-vsa1
- starent-vsa1-835
- custom9

mcc mcc_id: The mobile country code. This must be specified as a string of integers from 001 through 999. Values must be expressed as three integers.
mnc mnc_id: The mobile network code. This must be specified as a string of integers from 01 through 999. Values must be expressed as a minimum of two integers and a maximum of three integers.

contact who

Default: No contact specified.
contact who specifies the contact information for the chassis. who must be a string of 0 to 255 characters. The string specified must be embedded in double quotes (") if spaces and special punctuation is to be used.
hostname host_name

hostname host_name: configures the chassis host name where host_name must be from 1 to 63 characters.

Important: Please note that changing the chassis host name results in the command prompt changing as well to reflect the new name. This may affect any scripted interfaces from OSS or maintenance facility.

location text

Default: No location specified.

location text: specifies the location text to use which may be a string of 0 to 255 characters. The text specified must be embedded in double quotes ("") if spaces are to be used.

Usage
Specify system basic information which is useful back at a network operations center which uses the SNMP interfaces for management.

Example
The following commands configure the contact information, system host name, and location text, or remove configured location and system respectively.

    system contact user1@company.com
    system hostname system16
    system location "Clark Street Closet\nBasement Rack 4"

The following commands remove the configured contact and location from system respectively

    default system contact
    default system location
task facility ipsecmgr

Configures IPSec manager settings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
task facility ipsecmgr { max-crypto-maps-each-ipsecmgr max_num | max-ipsecmgr-tasks max_num | start-at-a-time num | task-count { increased | normal }}
```

default task facility ipsecmgr { max-crypto-maps-each-ipsecmgr max_num | max-ipsecmgr-tasks max_num | start-at-a-time num | task-count normal }

| max-crypto-maps-each-ipsecmgr max_num |
Default: 2
The maximum number of crypto maps per IPSEC manager.
max_num must be an integer from 1 through 150.

| max-ipsecmgr-tasks max_num |
Default: 200
The maximum number of IPSEC manager tasks that can be started for all services.
max_num must be an integer from 1 through 200.

| start-at-a-time num |
Default: 1
The number of IPSEC manager tasks created at once when they are required.
num must be an integer from 1 to 128.

| task-count { increased | normal } |
Default: normal
Adjusts the IPSec manager task count to support EHA.
**increased**: Increases the number of IPSec manager tasks operating on the PSCs/PSC2s while reducing the number of session manager tasks.
**normal**: Uses the standard algorithm for allocation memory for IPSec manager tasks.

**Caution**: If **task-count** is set to **normal** and session-recovery is enabled, IPSecMgr tasks are not allowed to start on most PSCs/PSC2s.

**Usage**
Set the IPSec manager parameters for all IPSec managers in the system.
Example
Use the following command to set the maximum number of crypto maps per IPSec manager to 25:

```
task facility ipsecmgr max-crypto-maps-each-ipsecmgr 25
```
task facility sessmgr

Configures system information which is accessible via SNMP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

task { facility sessmgr start { aggressive | normal } | resource cpu-memory-low { kill | warn } }

facility sessmgr start { aggressive | normal }

Default: Normal
Specifies the facility options for the session manager.

aggressive: specifies the maximum number of session manager processes are started immediately.

⚠️ Caution: The task facility sessmgr start aggressive command should only be used if the system will reach capacity (for the existing configuration) during the first few minutes of service.

⚠️ Caution: This command must only be executed last during configuration (or appended to the end of the configuration file) to ensure the availability of memory resources to contexts and services.

normal: indicates the session manager processes are started as needed.

resource cpu-memory-low { kill | warn }

Default: kill
Sets the action for the Resource Manager to take when the amount of free memory on a CPU falls below 12MB. An SNMP TRAP and CORBA notification are generated and the event is logged.
Once the free memory threshold is crossed, the Resource Manager examines all tasks on that CPU and finds the most over limit task and kills it. If there are no over limit tasks nothing happens. Resource Manager takes preference on killing a non-sessmgr task over a sessmgr task.

kill: The task most over memory limit (if any) is killed and recovered.
warn: The event is logged and no tasks are killed.

Usage

Set the session manager start policy to aggressive on heavily utilized systems to avoid undue delays in processing subscriber sessions.
Set the CPU memory low action to only log CPU low memory events.

Example

task facility sessmgr start aggressive
task facility sessmgr start normal

task resource cpu-memory-low warn
task facility acsmgr

This command configures the ACSMgr tasks setting.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

task facility acsmgr start [ aggressive | normal ]

no task facility acsmgr start

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Disables the configured ACSMgr setting.

<table>
<thead>
<tr>
<th>aggressive</th>
</tr>
</thead>
</table>
| Specifies to start the maximum possible ACSMgr tasks.

<table>
<thead>
<tr>
<th>normal</th>
</tr>
</thead>
</table>
| Configures the resource subsystem to start/stop ACSMgr tasks on as needed basis.

Usage
This command provides option for the resource subsystem to start maximum possible ACSMgr tasks based on the license configured and the available system configuration.

Example
The following command starts the maximum possible ACSMgr tasks:

```plaintext
task facility acsmgr start aggressive
```
Global Configuration Mode Commands

terminal

Configures the console port on the SPIO.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
terminal { carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware {off | on } | none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 | 9600 } | stopbits { 1 | 2 } }
```

carrierdetect { off | on }

Specifies whether or not the console port is to use Data Carrier Detect (DCD) when connecting to a terminal.
Default: off
off: Do not use DCD
on: Use DCD

databits { 7 | 8 }

Specifies the number of data bits used to transmit and receive characters.
Default: 8
7: Use 7 databits to transmit and receive characters.
8: Use 8 databits to transmit and receive characters.

flowcontrol { hardware {off | on } | none }

Specifies how the flow of data is controlled between the SPIO and a terminal.
Default: none
hardware: Enable or disable the use of hardware-based flow control
off: Disable the use of Ready to Send (RTS) and Clear to Send (CTS).
on: Enable the use of Ready to Send (RTS) and Clear to Send (CTS).
none: Disable the use of DCD, RTS and CTS.

parity { even | none | odd }

Specifies the type of error checking used on the port.
Default: none
even - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.
none - Disables error checking.
odd - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

speed { 115200 | 19200 | 38400 | 57600 | 9600 }

Specifies the flow of data in bits per second between the console port and terminal.
Default: 9600
stopbits { 1 | 2 }

Specifies the number of stop bits between each transmitted character.
Default: 1
  1: Use one stop bit between each transmitted character.
  2: Use two stop bits between each transmitted character.

Usage

Sets the SPIO’s console port parameters for communication with the terminal device.

Example

The following command sets the SPIO’s console port. The terminal must support these values.

```
terminal carrierdetect off databits 7 flowcontrol hardware on parity even speed 115200 stopbits 1
```
threshold

The commands in this section set global thresholding parameters.
threshold 10sec-cpu-utilization

Configures a threshold that measures a 10 second average of cpu utilization. Its polling interval can be set down to 30 seconds.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

```
threshold 10sec-cpu-utilization percent [ clear percent ]
```

**percent**
Default: 0
Configures the high threshold for 10 second average cpu-utilization. If the monitored CPU utilization is greater than or equal to the specified percentage an alert is sent. Regardless of the length of the polling interval, only one sample at the end of the polling interval is tested.

**clear percent**
Default: 0:
This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Use this command to set a threshold that sends an alert when CPU utilization over a 10 second average exceeds the limit set.
Alerts or alarms are triggered for 10-second sample of CPU utilization based on the following rules:

- **Enter condition**: 10-second average percentage of CPU utilization ≥ High Threshold
- **Clear condition**: 10-second average percentage of CPU utilization < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

**Important**: This command is not supported on all platforms.

**Example**
Send an alert when the 10 second average CPU utilization reaches 45 percent by entering the following command:
threshold 10sec-cpu-utilization 45
threshold aaa-acct-archive-size

This command configures accounting message archive size threshold.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

```
threshold aaa-acct-archive-size high_thresh [ clear low_thresh ]
```

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 1</td>
</tr>
<tr>
<td>The high threshold number of archived accounting messages that must be met or exceeded within the polling interval to generate an alert or alarm.</td>
</tr>
<tr>
<td>The number can be configured to any integer value between 0 and 1044000.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 1</td>
</tr>
<tr>
<td>The low threshold number of archived accounting messages that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td>The number can be configured to any integer value between 0 and 1044000.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.

Accounting message archive size thresholds generate alerts or alarms based on the number of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition:** Actual number of archived messages ≥ High Threshold
- **Clear condition:** Actual number of archived messages < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a high threshold count of 250 AAA accounting archived messages and low threshold of 100 for an system using the Alarm thresholding model:

```
threshold aaa-acct-archive-size 250 clear 100
```
threshold aaa-acct-failure

Configures accounting failure thresholds for the system.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

threshold aaa-acct-failure high_thres [ clear low_thres ]

**high_thres**
Default: 0
The high threshold number of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**clear low_thres**
Default: 0
The low threshold number of accounting failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Accounting failure thresholds generate alerts or alarms based on the number of failed AAA accounting message requests that occur during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.
Alerts or alarms are triggered for accounting failures based on the following rules:
- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a high threshold count of 100 AAA accounting failures and low threshold of 25 for an system using the Alarm thresholding model:
threshold aaa-acct-failure 100 clear 25
threshold aaa-acct-failure-rate

Configures accounting failure rate thresholds for the system.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

threshold aaa-acct-failure-rate high_thresh [ clear low_thresh ]

- **high_thresh**
  - Default: 1
  - The high threshold percent of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm.
  - high_thresh can be configured to any integer value between 0 and 100.

- **clear low_thresh**
  - Default: 1
  - The low threshold percent of accounting failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - low_thresh can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Accounting failure rate thresholds generate alerts or alarms based on the percentage of AAA accounting message requests that failed during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failure rates based on the following rules:

- **Enter condition:** Actual failure percentage \( \geq \) High Threshold
- **Clear condition:** Actual failure percentage \(< \) Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a AAA accounting failure rate high threshold percentage of 30 and a low threshold percentage of 10 for an system using the Alarm thresholding model:
threshold aaa-acct-failure-rate 30 clear 10
threshold aaa-auth-failure

Configures authentication failure thresholds for the system.

**Product**
PDSN, GGSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold aaa-auth-failure high_thresh [ clear low_thresh ]
```

<table>
<thead>
<tr>
<th><strong>high_thresh</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm. The number can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>clear low_thresh</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. The number can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Authentication failure thresholds generate alerts or alarms based on the number of failed AAA authentication message requests that occur during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with. Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a high threshold count of 100 AAA authentication failures for an system using the Alert thresholding model:

```
threshold aaa-auth-failure 100
```
threshold aaa-auth-failure-rate

Configures authentication failure rate thresholds for the system.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax
threshold aaa-auth-failure-rate high_thresh [ clear low_thresh ]

**high_thresh**
Default: 5
The high threshold percent of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh can be configured to any integer value between 0 and 100.

**clear**
Allows the configuration of the low threshold.

**low_thresh**
Default: 5
The low threshold percent of authentication failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Authentication failure rate thresholds generate alerts or alarms based on the percentage of AAA authentication message requests that failed during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with. Alerts or alarms are triggered for authentication failures based on the following rules:
- **Enter condition:** Actual failure percentage ≥ High Threshold
- **Clear condition:** Actual failure percentage < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a AAA authentication failure rate high threshold percentage of 30 for an system using the Alert thresholding model:

```
threshold aaa-auth-failure-rate 30
```
**threshold aaa-retry-rate**

Configures AAA retry rate thresholds for the system.

**Product**

PDSN, GGSN, HA, ASN GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
threshold aaa-retry-rate [high_thresh] [clear low_thresh]
```

**high_thresh**

Default: 5

The high threshold percent of AAA request message retries that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh can be configured to any integer value between 0 and 100.

**clear low_thresh**

Default: 5

The low threshold percent of AAA request message retries that maintains a previously generated alarm condition. If the percentage of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh can be configured to any integer value between 0 and 100.

---

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

---

**Usage**

AAA request message retry rate thresholds generate alerts or alarms based on the percentage of request messages (both authentication and accounting) that were retried during the specified polling interval. The percentage is based on a message count taken for all AAA authentication and accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for request message retries based on the following rules:

- **Enter condition:** Actual retry percentage ≥ High Threshold
- **Clear condition:** Actual retry percentage < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

---

**Example**

The following command configures a AAA message retry rate high threshold percentage of 25 and a low threshold percentage of 10 for an system using the Alarm thresholding model:
threshold aaa-retry-rate 25 clear 10
threshold aaamgr-request-queue

This command configures the AAA Manager internal request queue threshold.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

threshold aaamgr-request-queue high_thresh [ clear ] low_thresh

high_thresh
Default: 0
The high threshold number of AAA Manager Requests that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh can be configured to any integer value between 1 and 100.

clear
Allows the configuration of the low threshold.

low_thresh
Default: 5
The low threshold number of AAA Manager Requests that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm is generated.
low_thresh can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
AAA Manager Request thresholds generate alerts or alarms based on the number of AAA Manager Requests for an AAA manager process during the specified polling interval.
Alerts or alarms are triggered for AAA Manager Requests based on the following rules:

- **Enter condition:** Actual number of AAA Manager Requests per AAA manager ≥ High Threshold
- **Clear condition:** Actual number of AAA Manager Requests per AAA manager process < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm is not generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
Example
The following command configures a AAA authentication failure rate high threshold percentage of 30 for a system using the Alert thresholding model:

```plaintext
threshold aaamgr-request-queue 30
```
threshold asngw-auth-failure

Configures authentication failure thresholds for the ASN-GW system.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```
threshold asngw-auth-failure high_thresh [ clear low_thresh ]
```

default threshold asngw-auth-failure

```
high_thresh
Default: 0
The high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.
```

```
clear low_thresh
Default: 0
The low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.
```

```
| Important: | This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold. |
```

Usage

Use this command to configure threshold limits to generate alerts or alarms based on the number of failed ASN-GW authentication message requests that occur during the specified polling interval. Authentication requests are counted for all ASN Gateway authentication servers that the system is configured to communicate with.

Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures a high threshold count of 100 authentication failures for an ASN-GW using the Alert thresholding model:

```
threshold asngw-auth-failure 100
```
threshold asngw-handoff-denial

Configures thresholds for hand-off denial for the ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold asngw-handoff-denial high_thresh[ clear low_thresh]
default threshold asngw-handoff-denial
```

**high_thresh**
Default: 0
The high threshold number of hand-off denials that must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thresh` can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of hand-off denials that maintains a previously generated alarm condition. If the number of hand-off denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set threshold limits to generate alerts or alarms based on the number of denied hand-off that occurred during the specified polling interval. Hand-off denial messages are counted for all ASN Gateways that the system is configured to communicate with.
Alerts or alarms are triggered for hand-off denials based on the following rules:
- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures a high threshold count of 100 hand-off denials using the Alert thresholding model:

```
threshold asngw-handoff-denial 100
```
**threshold asngw-max-eap-retry**

Configures thresholds for maximum retries for Extensible Authentication Protocol (EAP) authentication on an ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold asngw-max-eap-retry high_thresh[ clear low_thresh]
default threshold asngw-max-eap-retry
```

**high_thresh**
Default: 0
The high threshold number of retries for EAP authentication that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of retries for EAP authentication that maintains a previously generated alarm condition. If the number of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Use this command to set threshold limits to generate alerts or alarms based on the number of retries for EAP authentication that occur during the specified polling interval. Alerts or alarms are triggered for maximum number of retries for EAP authentication based on the following rules:

- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures a high threshold count of 100 alerts or alarms generated on maximum number of retries for EAP authentication for an ASN Gateway using the Alert thresholding model:

```
threshold asngw-handoff-denial 100
```
**threshold asngw-network-entry-denial**

Configures thresholds for denial of network entry to an MS with in the ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold asngw-network-entry-denial high_thresh [ clear low_thresh ]
```

default threshold asngw-network-entry-denial

```
high_thresh

Default: 0
The high threshold number of denial of network entry to an MS that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.
```

```
clear low_thresh

Default: 0
The low threshold number of denial of network entry to an MS that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set threshold limits to generate alerts or alarms based on the number of network entry denials that occurred during the specified polling interval. Network denial messages are counted for an MS that the system is configured to communicate with. Alerts or alarms are triggered for network entry denials based on the following rules:

- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures a high threshold count of 100 network entry denials for an MS using the Alert thresholding model:

```
threshold asngw-network-entry-denial 100
```
threshold asngw-r6-invalid-nai

Configures thresholds to generate alert/alarm for invalid Network Access Identifier (NAI) in R6 message.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```
threshold asngw-r6-invalid-nai high_thresh [ clear low_thresh ]
default threshold asngw-r6-invalid-nai
```

**high_thresh**
Default: 0
The high threshold number of invalid NAIs in R6 messages that must be met or exceeded within the polling interval to generate an alert or alarm. 
`high_thresh` can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of invalid NAIs in R6 messages that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated. 
`low_thresh` can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Use this command to set threshold limits to generate alerts or alarms based on the number of invalid NAIs in R6 messages that occurred during the specified polling interval. Invalid NAIs are counted for an MS that the system is configured to communicate with or per system for all R6 messages. 
Alerts or alarms are triggered for invalid NAIs based on the following rules:
- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. 
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures a high threshold count of 100 invalid NAIs in R6 messages using the Alert thresholding model:

    threshold asngw-r6-invalid-nai 100
threshold asngw-session-setup-timeout

Configures thresholds to generate alert/alarm for session setup timeouts in an ASN-GW service.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```plaintext
threshold asngw-session-setup-timeouthigh_thresh[ clearlow_thresh]
default threshold asngw-session-setup-timeout
```

### high_thresh

Default: 0
The high threshold number of timeouts during session setup that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

### clear low_thresh

Default: 0
The low threshold number of timeouts during session setup that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

> **Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.

Alerts or alarms are triggered for session setup timeouts based on the following rules:

- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a high threshold count of 100 timeouts during session setup using the Alert thresholding model:

```
threshold asngw-session-setup-timeout 100
```
threshold asngw-session-timeout

Configures thresholds to generate alert/alarm for session timeouts in an ASN-GW service.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```
threshold asngw-session-timeout high_thresh [ clear low_thresh ]
default threshold asngw-session-timeout
```

```
high_thresh
Default: 0
The high threshold number of timeouts during session that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
The low threshold number of timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh can be configured to any integer value between 0 and 10000000. A value of 0 disables the threshold.
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during a session that occurred during the specified polling interval. Alerts or alarms are triggered for session timeouts based on the following rules:

- **Enter condition:** Actual number of failures ≥ High Threshold
- **Clear condition:** Actual number of failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

```
```
The following command configures a high threshold count of 100 timeouts during a session using the Alert thresholding model:

```
threshold asngw-session-timeout 100
```
threshold call-reject-no-resource

Configures thresholds on the system for calls rejected due to insufficient resources.

Product
All

Privilege
Security Administrator, Administrator

Syntax

threshold call-reject-no-resource high_thresh [ clear low_thresh ]

high_thresh

Default: 0
The high threshold number of no-resource call rejects issued by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

clear low_thresh

Default: 0
The low threshold number of no-resource call rejects issued by the system that maintains a previously generated alarm condition. If the number of rejections falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

No resource call reject thresholds generate alerts or alarms based on the total number of calls that were rejected by the system due to insufficient or no resources (memory and/or session licenses) during the specified polling interval.
Alerts or alarms are triggered for no-resource-rejected calls based on the following rules:

- **Enter condition:** Actual number of calls rejected due to no resources ≥ High Threshold
- **Clear condition:** Actual number of calls rejected due to no resources < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a high threshold count for the number of calls rejected by the system due to insufficient or no resources to 100 and allow threshold of 40 for an system using the Alarm thresholding model:

```
threshold call-reject-no-resource 100 clear 40
```
threshold call-setup

Configures call setup thresholds for the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold call-setup high_thresh[ clear low_thresh]
```

**high_thresh**
Default: 0
The high threshold number of calls setup by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of calls setup by the system that maintains a previously generated alarm condition.
If the number of setups falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Call setup thresholds generate alerts or alarms based on the total number of calls setup by the system during the specified polling interval.
Alerts or alarms are triggered for call setups based on the following rules:
- **Enter condition:** Actual number of call setups \( \geq \) High Threshold
- **Clear condition:** Actual number of call setups < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll monitoring` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a high threshold count of 100 calls setup for an system using the Alert thresholding model:
threshold call-setup 100
threshold call-setup-failure

Configures call setup failure thresholds for the system.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
threshold call-setup-failure [high_thresh] [clear low_thresh]
```

**high_thresh**

Default: 0  
The high threshold number of call setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.  
The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0  
The low threshold number of call setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.  
The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Call setup failure thresholds generate alerts or alarms based on the total number of call setup failures experienced by the system during the specified polling interval.  
Alerts or alarms are triggered for call setup failures based on the following rules:

- **Enter condition**: Actual number of call setup failures ≥ High Threshold  
- **Clear condition**: Actual number of call setup failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.  
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 call setup failures and a low threshold of 80 for an system using the Alarm thresholding model:
threshold call-setup-failure 100 clear 80
threshold cpu-available-memory

Configures thresholds for available CPU memory for the system.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
threshold cpu-available-memory low_thresh [ clear high_thresh ]
```

<table>
<thead>
<tr>
<th>low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 32</td>
</tr>
<tr>
<td>The low threshold amount of CPU memory that must be met or exceeded at the polling time to generate an alert or alarm.</td>
</tr>
<tr>
<td><code>low_thresh</code> is measured in mega bytes (MB) and can be configured to any integer value between 0 and 2048.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 32</td>
</tr>
<tr>
<td>The high threshold amount of CPU memory that maintains a previously generated alarm condition. If the memory amount rises above the high threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td><code>high_thresh</code> is measured in mega bytes (MB) and can be configured to any integer value between 0 and 2048.</td>
</tr>
</tbody>
</table>

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**

CPU available memory thresholds generate alerts or alarms based on the amount of available memory for each PSC/PSC2 CPU at the polling time. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for available CPU memory based on the following rules:

- **Enter condition**: Average measured amount of memory/CPU for last 5 minutes £ Low Threshold
- **Clear condition**: Average measured amount of memory/CPU for last 5 minutes > High Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important**: This command is not supported on all platforms.
Example
The following command configures a low threshold count of 50 MB CPU memory available and a high threshold of 112 MB for an system using the Alarm thresholding model:

```
threshold cpu-available-memory 50 clear 112
```
threshold cpu-load

Configures the threshold for monitoring PSC/PSC2 CPU loads using a 5 minute average measurement. The threshold is enabled by enabling CPU resource monitoring.

Product
All

Privilege
Security Administrator, Administrator

Syntax

threshold cpu-load high_thresh [ clear low_thresh ]

- high_thresh
  Default: 0
  If the monitored CPU load is greater than or equal to the specified number an alert is sent. high_thresh must be an integer from 0 through 15.

- clear low_thresh
  Default: 0
  This is a low watermark value that sets the alarm clearing threshold value. If not present it is taken from the first value. low_thresh must be an integer from 0 through 15.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert when the card’s CPU load is equal to or greater than the number specified. Alerts or alarms are triggered for CPU load based on the following rules:
- Enter condition: Actual CPU load ≥ High Threshold
- Clear condition: Actual CPU load < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

To set an alert when the PSC/PSC2 CPU load is over 10 and set an alert clear when the CPU load drops down equal or less than 7, enter the following command;

threshold cpu-load 10 clear 7
threshold cpu-memory-usage

Configures the threshold for monitoring the percentage of total CPU memory used during the polling interval.

Product
All

Privilege
Security Administrator, Administrator

Syntax

threshold cpu-memory-usage high_thresh [ clear low_thresh ]

 high_thresh
Default: 0
The high threshold for percentage of total memory used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.
high_thresh is measured in percentage of total CPU memory used and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

clear low_thresh
Default: 0
The low threshold for percentage of total CPU memory used that maintains a previously generated alarm condition. If the memory usage falls below the low threshold within the polling interval, a clear alarm is generated.
low_thresh is measured in percentage of total CPU memory used and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

CPU memory usage generate alerts or alarms based on the percentage of total CPU memory used during the polling interval.
Alerts or alarms are triggered for CPU memory usage session based on the following rules:

• Enter condition: Actual percentage of CPU memory usage ≥ specified percentage of total CPU memory.

• Clear condition: Actual CPU memory usage < specified clear percentage of total CPU memory usage.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a threshold of 65 percent of total PSC/PSC2 CPU memory usage and a clear threshold of 35 percent:

```
threshold cpu-memory-usage 65 clear 35
```
threshold cpu-orbs-crit

Configures threshold for generating critical-level alerts or alarms based on the percentage of CPU utilization by the ORBS software task

Product
All

Privilege
Security Administrator, Administrator

Syntax

threshold cpu-orbs-crit [default]
high_thresh [clear low_thresh]

default
Restores this parameter to its default setting.

high_thresh
Default: 60
The high threshold percent of CPU utilization by the ORB software task that must be exceeded as measured at the time of polling to generate a critical-level alert or alarm.
high_thresh is measured in percentage of total CPU utilization and can be configured to any integer value 0 through 100. A value of 0 disables the threshold.

clear low_thresh
Default: 60
The low threshold percent of CPU utilization by the ORB software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to the low threshold at the time of polling, a clear alarm will be generated.
low_thresh is measured in percentage of total CPU utilization and can be configured to any integer value 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage
Object Request Broker (ORB) software task CPU utilization thresholds generate critical-level alerts or alarms based on the percentage of SMC CPU resources it is consuming at the time of polling.
Critical-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

• Enter condition: Actual CPU usage percentage > High Threshold
• Clear condition: Actual CPU usage percentage £ Low Threshold

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
**Example**
The following command configures a critical-level alarm threshold of 35 percent of CPU utilization by the ORBS task and a clear threshold of 35 percent:

```plaintext
threshold cpu-orbs-crit 35 clear 35
```
threshold cpu-orbs-warn

Configures threshold for generating warning-level alerts or alarms based on the percentage of CPU utilization by the ORBS software task.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold cpu-orbs-warn high_thresh[ clear low_thresh]
[ default ] threshold cpu-orbs-warn
```

**default**
Restores this parameter to its default setting.

**high_thresh**
Default: 50
The high threshold percent of CPU utilization by the ORB software task that must be exceeded as measured at the time of polling to generate a warning-level alert or alarm.

`high_thresh` is measured in percentage of total CPU utilization and can be configured to any integer value 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**
Default: 50
The low threshold percent of CPU utilization by the ORB software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to the low threshold at the time of polling, a clear alarm will be generated.

`low_thresh` is measured in percentage of total CPU utilization and can be configured to any integer value 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**
Object Request Broker (ORB) software task CPU utilization thresholds generate warning-level alerts or alarms based on the percentage of SMC CPU resources it is consuming at the time of polling.

Warning-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage > High Threshold
- **Clear condition:** Actual CPU usage percentage £ Low Threshold

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures a warning-level alarm threshold of 25 percent of CPU utilization by the ORBS task and a clear threshold of 25 percent:

```
threshold cpu-orbs-warn 25 clear 25
```
**threshold cpu-session-throughput**

Configures thresholds for CPU session throughput for the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
threshold cpu-session-throughput high_thres [ clear low_thres ]
```

**high_thres**

Default: 0
The high threshold session throughput that must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thres` is measured in Kilobytes per second (Kbps) and can be configured to any integer value between 0 and 1000000000. A value of 0 disables the threshold.

**clear low_thres**

Default: 0
The low threshold session throughput that maintains a previously generated alarm condition. If the throughput falls below the low threshold within the polling interval, a clear alarm will be generated.
`low_thres` is measured in Kilobytes per second (Kbps) and can be configured to any integer value between 0 and 1000000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

CPU session throughput thresholds generate alerts or alarms based on total throughput for all Session Manager tasks running on each PSC/PSC2 CPU during the polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for CPU session throughput based on the following rules:

- **Enter condition:** Actual CPU session throughput \( \geq \) High Threshold
- **Clear condition:** Actual CPU session throughput < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.
Example
The following command configures a high threshold count of 900 Kbps session throughput and a low threshold of 500 KBps for a system using the Alarm thresholding model:

```
threshold cpu-session-throughput 900 clear 500
```
threshold cdr-file-space

Configures the threshold for monitoring the percentage of total file space allocated for CDRs used during the polling interval.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
threshold cdr-file-space high_thresh [ clear low_thresh ]
default threshold cdr-file-space
```

default
Configures the default setting.

```
high_thresh
```

Default: 90
The high threshold for percentage of total allocated CDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm. *high_thresh* is measured in percentage of total allocated CDR file space used and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

```
clear low_thresh
```

Default: 0
The low threshold for percentage of total allocated CDR file space used that maintains a previously generated alarm condition. If the space usage falls below the low threshold within the polling interval, a clear alarm is generated. *low_thresh* is measured in percentage of total allocated CDR file space used and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

CDR file space usage generate alerts or alarms based on the percentage of total allocated CDR file space used during the polling interval.

Alerts or alarms are triggered for CDR file space usage session based on the following rules:

- **Enter condition:** Actual percentage of allocated CDR file space usage \( \geq \) specified percentage of total CDR file space.
- **Clear condition:** Actual CDR file space used < specified clear percentage of total allocated CDR file space usage.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a threshold of 65 percent of total allocated CDR file space usage and a clear threshold of 35 percent:

```
threshold cdr-file-space 65 clear 35
```
threshold contfilt-block

Configures the threshold for Content Filtering rating operations blocked during a polling interval at which the threshold are raised or cleared.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
threshold contfilt-block high_thresh_value [ clear low_thresh_value ]
default threshold contfilt-block
```

**high_thresh**

Default: 90
The high threshold for number of rating operations blocked for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

*high_thresh* is measured in numbers of total rating operations blocked and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
The low threshold for the total number of rating operations blocked for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below the low threshold within the polling interval, a clear alarm is generated.

*low_thresh* is measured in number of total rating operations blocked and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**Usage**

Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations blocked for a content filtering service during the polling interval. If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll contfilt-block` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a threshold of 65 percent of total rating operations blocked and a clear threshold of 35 percent:

```
threshold contfilt-block 65 clear 35
```
threshold contfilt-rating

Configures the threshold for Content Filtering rating operations performed during a polling interval at which the threshold are raised or cleared.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold contfilt-rating high_thresh_value [ clear low_thresh_value ]
default threshold contfilt-rating
```

**high_thresh**
Default: 90
The high threshold for number of rating operations performed for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

**clear low_thresh**
Default: 0
The low threshold for the total number of rating operations performed for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below the low threshold within the polling interval, a clear alarm is generated.

**Usage**
Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations performed for a content filtering service during the polling interval. If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll contfilt-rating` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a threshold of 65 percent of total rating operations performed and a clear threshold of 35 percent:

```
threshold contfilt-rating 65 clear 35
```
threshold cpu-utilization

Configures thresholds for CPU utilization for the system.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
threshold cpu-utilization high_thresh [ clear low_thresh ]
```

- **high_thresh**
  - Default: 85
  - The high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` can be configured to any integer value between 0 and 100.

- **clear low_thresh**
  - Default: 85
  - The low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
  - `low_thresh` can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each PSC/PSC2 CPU during the specified polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU. Alerts or alarms are triggered for CPU utilization based on the following rules:

- **Enter condition:** Average measured CPU utilization for last 5 minutes ≥ High Threshold
- **Clear condition:** Average measured CPU utilization for last 5 minutes < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**

```
```

Cisco ASR 5000 Series Command Line Interface Reference
The following command configures a high threshold CPU utilization percentage of 90 for an system using the Alert thresholding model:

```
threshold cpu-utilization 90
```
threshold dcca-bad-answer

Configures the threshold for invalid or bad responses to the system from Diameter server.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ default ] threshold dcca-bad-answer high_thres [ clear low_thres ]

default
Disables the threshold for configured alarm and set the high_thres and low_thres values to 0.

high_thres
Default: 0
The high threshold number of invalid messages or responses that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value between 0 and 1044000.

clear low_thres
Default: 0
The low threshold number of invalid messages/responses that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 1044000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
In the event that the system receives invalid message or response from Diameter server dcca-bad-answer is generated.
DCCA bad answer messages size threshold generates alerts or alarms based on the number of invalid response or messages received during the specified polling interval.
Alerts or alarms are triggered for DCCA bad answers based on the following rules:

● Enter condition: Actual number of DCCA bad answer messages ≥ High Threshold

● Clear condition: Actual number of DCCA bad answer messages < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Example
The following command configures a high threshold count of 250 DCCA bad answer messages and low threshold of 100 for an system using the Alarm thresholding model:

```
threshold dcca-bad-answer 250 clear 100
```
threshold dcca-protocol-error

Configures the threshold for Diameter Credit Control Application (DCCA) protocol error from Diameter server.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ default ] threshold dcca-protocol-error high_thresh [ clear low_thresh ]

default
Disables the threshold for configured alarm and sets the high_thresh and low_thresh values to 0.

high_thresh
Default: 0
The high threshold number of protocol error received from Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value between 0 and 1044000.

clear low_thresh
Default: 0
The low threshold number of protocol error received from Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 1044000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
In the event that the system receives the protocol errors from Diameter server, dcca-protocol-error is generated.
DCCA protocol error threshold generates alerts or alarms based on the number of protocol error messages received from Diameter server during the specified polling interval.
Alerts or alarms are triggered for DCCA protocol error based on the following rules:

• Enter condition: Actual number of DCCA protocol error ≥ High Threshold

• Clear condition: Actual number of DCCA protocol errors < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Example
The following command configures a high threshold count of 250 protocol errors and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-protocol-error 250 clear 100
```
threshold dcca-rating-failed

Configures Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject thresholds.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ default ] threshold dcca-rating-failed high_thresh [ clear low_thresh ]

default
Disables the threshold for configured alarm and sets the high_thres and low_thres values to 0.

high_thresh
Default: 0
The high threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value between 0 and 1044000.

clear low_thresh
Default: 0
The low threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 1044000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the Diameter server rejects the system request for a block of credits due to invalid Rating Group, defined as content-id, dcca-rating-failed message is generated.
Rating Group failed threshold generates alerts or alarms based on the number of requests rejected from Diameter server during the specified polling interval.
Alerts or alarms are triggered for Rating Group failed based on the following rules:

- Enter condition: Actual number of DCCA Rating Group failed ≥ High Threshold
- Clear condition: Actual number of DCCA Rating Group failed < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Example
The following command configures a high threshold count of 250 requests rejected and low threshold of 100 for an system using the Alarm thresholding model:

```
threshold dcca-rating-failed 250 clear 100```

threshold dcca-unknown-rating-group

Configures the unknown Diameter Credit Control Application (DCCA) Rating Group (content-id) returned by Diameter to system thresholds.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
[ default ] threshold dcca-unknown-rating-group high_thresh [ clear low_thresh ]
```

**default**
Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

**high_thresh**
Default: 0
The high threshold number of unknown Rating Group (content-id) sent by Diameter server and received by system that must be met or exceeded within the polling interval to generate an alert or alarm. The number can be configured to any integer value between 0 and 1044000.

**clear low_thresh**
Default: 0
The low threshold number of unknown Rating Group (content-id) sent by Diameter server and received by system that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated. The number can be configured to any integer value between 0 and 1044000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
In the event that the Diameter server sends invalid Rating Groups, **content-ids** to the system, **dcca-unk-rating-group** message is generated.
Unknown Rating Group threshold generates alerts or alarms based on the number of unknown Rating Groups received by the system from Diameter server during the specified polling interval. Alerts or alarms are triggered for unknown rating groups based on the following rules:

- **Enter condition:** Actual number of unknown rating groups \( \geq \) High Threshold
- **Clear condition:** Actual number of unknown rating groups \( < \) Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Example
The following command configures a high threshold count of 250 unknown rating groups and low threshold of 100 for an system using the Alarm thresholding model:

```
threshold dcca-unknown-rating-group 250 clear 100
```
threshold diameter diameter-retry-rate

This command configures Diameter Retry Rate threshold for generating alerts or alarms based on the percentage of Diameter requests that were retried during the polling interval.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold diameter diameter-retry-rate high_thresh [ clear low_thresh ]
default threshold diameter diameter-retry-rate
```

**default**
Configures the default setting.
Default: Disables the thresholds; the threshold values are reset to 0.

```
high_thresh
```

Default: 0
Specifies the high threshold. If, within the polling interval, the percentage of Diameter requests retried equals or exceeds `high_thresh`, an alert or alarm is generated.
`high_thresh` must be an integer from 0 through 100.

```
clear low_thresh
```

Default: 0
Specifies the low threshold. If, within the polling interval, the percentage of Diameter requests retried falls below `low_thresh`, a clear alarm is generated.
`low_thresh` must be an integer from 0 through 100.

**Important:** This value is applicable for the Alarm mode, and ignored for the Alert mode. In addition, if this value is not configured for the Alarm mode, the system assumes it is identical to the high threshold.

**Usage**
Diameter Retry Rate threshold generates alerts or alarms based on the percentage of Diameter requests that were retried during the specified polling interval.
Alerts or alarms are triggered based on the following rules:

- **Enter condition:** Percentage of Diameter requests retried > High Threshold
- **Clear condition:** Percentage of Diameter requests retried < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Example
The following command configures a high threshold of 75 percent, and a low threshold of 50 percent for a system using the Alarm thresholding model:

```
threshold diameter diameter-retry-rate 75 clear 50
```
threshold edr-file-space

Configures the threshold for monitoring the percentage of total file space allocated for EDRs used during the polling interval.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ default ] threshold edr-file-space high_thresh [ clear low_thresh ]

- **high_thresh**
  Default: 90
  The high threshold for percentage of total allocated EDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm. **high_thresh** is measured in percentage of total allocated EDR file space used and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  The low threshold for percentage of total allocated EDR file space used that maintains a previously generated alarm condition. If the space usage falls below the low threshold within the polling interval, a clear alarm is generated. **low_thresh** is measured in percentage of total allocated EDR file space used and can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

EDR file space usage generate alerts or alarms based on the percentage of total allocated EDR file space used during the polling interval. Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition:** Actual percentage of allocated EDR file space usage \( \geq \) specified percentage of total EDR file space.
- **Clear condition:** Actual EDR file space used < specified clear percentage of total allocated EDR file space usage.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.
Example
The following command configures a threshold of 65 percent of total allocated EDR file space usage and a clear threshold of 35 percent:

```
threshold edr-file-space 65 clear 35
```
### threshold edr-udr-dropped flow control

This command configures thresholds to monitor the total number of EDRs and UDRs discarded due to flow control.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
threshold edr-udr-dropped-flow-control high_thresh [ clear low_thresh ]
default threshold edr-udr-dropped-flow-control
```

- **default**
  
  Configures the default setting.
  
  Default: High threshold: 90; Low threshold: 10

- **high_thresh**
  
  Default: 90
  
  The high threshold for total number of EDRs + UDRs dropped due to flow control, which must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` must be an integer from 0 through 100000.
  
  A value of 0 indicates the threshold.

- **clear low_thresh**
  
  Default: 10
  
  The low threshold for total number of EDRs + UDRs dropped that maintains a previously generated alarm condition. If the total number of EDRs + UDRs dropped falls below the low threshold within the polling interval, a clear alarm is generated. `low_thresh` must be an integer from 0 through 100000, and must be lower than `high_thresh`.
  
  A value of 0 disables the threshold.

**Usage**

Use this command to configure thresholds to monitor the total number of EDRs + UDRs discarded due to flow control. Alerts or alarms are generated based on the total number of EDRs + UDRs dropped during polling interval.

Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition:** Actual number of EDRs + UDRs dropped >= specified number of EDRs + UDRs dropped.
- **Clear condition:** Actual number of EDR + UDRs dropped < specified clear number of EDRs + UDRs dropped.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures a high threshold of 90 and a clear threshold of 45 to monitor EDRs + UDRs dropped due to flow control:

```
threshold edr-udr-dropped-flow-control 90 clear 45
```
threshold fw-deny-rule

This command configures thresholds for Stateful Firewall Deny Rule.

Product
FW

Privilege
Security Administrator, Administrator

Syntax

threshold fw-deny-rule high_thresh [ clear low_thresh ]

default threshold fw-deny-rule

default
Disables the threshold and sets high_thresh and low_thresh to the default values.

high_thresh
Specifies the Stateful Firewall Deny-Rule threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear low_thresh
Specifies the Stateful Firewall Deny-Rule alarm clear threshold value. If, in the same polling interval, the threshold falls below low_thresh a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage
When the number of Deny-Rule exceeds a given value, a threshold is raised and it is cleared when the number of Deny-Rule fall below a value within the polling interval.
Refer to the threshold poll command to configure the polling interval, and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a Stateful Firewall Deny Rule high threshold of 1000 and a low threshold of 100 for a system using the Alarm Thresholding model:

threshold fw-deny-rule 1000 clear 100
threshold fw-dos-attack

This command configures thresholds for Stateful Firewall Denial-of-Service (DoS) attacks.

Product  
FW

Privilege  
Security Administrator, Administrator

Syntax

threshold fw-dos-attack high_thresh [ clear low_thresh ]

default threshold fw-dos-attack

default
Disables the threshold and sets high_thresh and low_thresh to the default values.

high_thresh
Specifies the Stateful Firewall DoS attacks threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear low_thresh
Specifies the Stateful Firewall DoS attacks clear threshold value. If, in the same polling interval, the threshold falls below low_thresh a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

When the number of DoS attacks exceed a given value, a threshold is raised and it is cleared when the number of DoS attacks fall below a value within the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example

The following command configures a Stateful Firewall DoS attacks high threshold of 1000 and a low threshold of 100 for a system using the Alarm Thresholding model:

threshold fw-dos-attack 1000 clear 100
threshold fw-drop-packet

This command configures thresholds for Stateful Firewall drop packets.

Product
FW

Privilege
Security Administrator, Administrator

Syntax
threshold fw-drop-packet high_thresh [ clear low_thresh ]

default threshold fw-drop-packet

default
Disables the threshold and sets high_thresh and low_thresh to the default values.

high_thresh
Specifies the Stateful Firewall drop packets threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear low_thresh
Specifies the Stateful Firewall drop packets clear threshold value. If, in the same polling interval, the threshold falls below low_thresh a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage
When the number of drop packets exceed a given value, a threshold is raised and it is cleared when the number of drop packets fall below a value within the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a Stateful Firewall drop packets high threshold of 1000 and a low threshold of 100 for a system using the Alarm thresholding model:

threshold fw-drop-packet 1000 clear 100
threshold fw-no-rule

This command configures thresholds for Stateful Firewall no rules.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold fw-no-rule high_thresh [ clear low_thresh ]
default threshold fw-no-rule
```

**default**

Disables the threshold and sets `high_thresh` and `low_thresh` to the default values.

**high_thresh**

Specifies the Stateful Firewall no rules threshold value, which if met or exceeded generates an alert or alarm. `high_thresh` must be an integer from 0 through 1000000.

Default: 0

**clear low_thresh**

Specifies the Stateful Firewall no rules clear threshold value. If, in the same polling interval, the threshold falls below `low_thresh` a clear alarm is generated.

`low_thresh` must be an integer from 0 through 1000000.

Default: 0

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**

When the number of no rules exceed a given value, a threshold is raised and it is cleared when the number of no rules fall below a value within the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a Stateful Firewall no rules high threshold of 1000 and a low threshold of 100 for a system using the Alarm Thresholding model:

```plaintext
threshold fw-no-rule 1000 clear 100
```
threshold license

Configures thresholds for session license utilization for the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] threshold license remaining-sessions low_thresh clear high_thresh
```

- **remaining-sessions low_thresh**
  - Default: 10
  - The low threshold session license utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `low_thresh` can be configured to any integer value between 0 and 100.

- **clear high_thresh**
  - Default: 10
  - The high threshold session license utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated.
  - `high_thresh` can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**

Session license utilization thresholds generate alerts or alarms based on the utilization percentage of all session capacity licenses during the specified polling interval.

As described in Chapter 7 of the Administration and Configuration Guide, the system uses session capacity license to dictate the maximum number of simultaneous sessions that can be supported. There are multiple session types that require licenses (i.e. Simple IP, Mobile IP, L2TP, etc.). Although, a single threshold is configured for all session types, alerts or alarms can be generated for each type.

Alerts or alarms are triggered for session license utilization based on the following rules:

- **Enter condition:** Actual session license utilization percentage per session type £ Low Threshold
- **Clear condition:** Actual session license utilization percentage per session type > High Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a session license low threshold percentage of 10 and a high threshold of 35 for an system using the Alarm thresholding model:

```
threshold license remaining-sessions 10 clear 35
```
threshold mgmt-cpu-memory-usage

Configures the thresholds for CPU memory usage.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold mgmt-cpu-memory-usage high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
The high threshold percent of CPU memory usage that must be met or exceeded within the polling interval to generate an alert or alarm. 
*high_thresh* is measured in percentage of total memory used and can be configured to any integer value 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**

The low threshold percent of CPU memory usage that maintains a previously generated alarm condition. If the percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is measured in percentage of total memory used and can be configured to any integer value 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

CPU memory usage thresholds generate alerts or alarms based on memory usage for the SMC CPU during the polling interval. A single threshold enables CPU monitoring for both the active and standby SMCs allowing for alerts or alarms to be generated for each CPU.
Alerts or alarms are triggered for SMC CPU memory usage based on the following rules:

- **Enter condition:** Actual CPU memory usage ≥ High Threshold
- **Clear condition:** Actual CPU memory usage < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**

This command is not supported on all platforms.
The following command configures a threshold of 65 percent of total SMC CPU memory usage and a clear threshold of 35 percent:

```
threshold mgmt-cpu-memory-usage 65 clear 35
```
threshold mgmt-cpu-utilization

Configures the thresholds for CPU utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold mgmt-cpu-utilization high_thres [ clear low_thres ]
```

- **high_thres**
  - Default: 0
  - The high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  - high_thres can be configured to any integer value between 0 and 100.

- **clear low_thres**
  - The low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - low_thres can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each SMC CPU during the specified polling interval. Although, a single threshold is configured for both SMC CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for SMC CPU utilization based on the following rules:

- **Enter condition:** Average measured CPU utilization for last 5 minutes ≥ High Threshold
- **Clear condition:** Average measured CPU utilization for last 5 minutes < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**
The following command configures a high threshold SMC CPU utilization percentage of 90 for an system using the Alert thresholding model:

```
threshold mgmt-cpu-utilization 90
```
threshold mme-attach-failure

Use this command to configure thresholds for the total number of MME Attach Failure messages to count across all the MME services in the system as threshold limit to generate alert or alarm.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold mme-attach-failure high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0 (Disabled)
The high threshold number of total MME Attach Failure messages across all MME services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 100000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0 (Disabled)
The low threshold number of total MME Attach Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages, across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to monitor and set alarms or alerts when the total number of MME Attach Failure message across all the MME services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of MME Attach Failure message based on the following rules:

- **Enter condition:** Actual total number of MME Attach Failure messages ≥ High Threshold
- **Clear condition:** Actual total number of MME Attach Failure messages < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll mme-attach-failure` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.
Example
The following command configures the limit of MME Attach Failure high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold mme-attach-failure 10000
```
**threshold mme-auth-failure**

Use this command to configure thresholds for the total number of MME Auth Failure messages to count across all the MME services in the system as threshold limit to generate alert or alarm.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold total-mme-auth-failure high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 0 (Disabled)
  The high threshold number of total MME Auth Failure messages across all MME services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
  The number can be configured to any integer value from 0 through 100000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0 (Disabled)
  The low threshold number of total MME Auth Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages, across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to monitor and set alarms or alerts when the total number of MME Auth Failure messages across all the MME services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of MME Auth Failure message based on the following rules:

- **Enter condition:** Actual total number of MME Auth Failure messages ≥ High Threshold
- **Clear condition:** Actual total number of MME Auth Failure messages < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll mme-auth-failure** command to configure the polling interval and the **threshold monitoring mme-service** command to enable thresholding for this value.
**Example**

The following command configures a total MME Auth Failure high threshold count of **10000** for an system using the Alert thresholding model:

```
threshold mme-auth-failure 10000
```
threshhold model

Configures the thresholding model for the system to use.

Product
All

Privilege
Security Administrator, Administrator

Syntax

threshold model { alarm | alert }

**alarm**
Selects the alarm thresholding model as described in the Usage section for this command.

**alert**
Selects the alert thresholding model as described in the Usage section for this command.

Usage

The system supports the following thresholding models:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded HT.

- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

The alarm is cleared at the end of the first interval where the measured value is below the low threshold.

In the example shown in the figure below, this model generates an alarm during period 2 when the count exceeds HT. A second alarm is generated in period 6 when the count falls beneath LT. The second alarm indicates a “clear” condition.
Figure 5. Thresholding Model Example

---

**Important:** Note that for certain values, the alert or alarm serves to warn of low quantities (i.e., memory, session licenses, etc.). In these cases, the low threshold is the condition that must be met or exceeded within the polling interval to generate the alert or alarm. Once the high threshold is exceeded during an interval, the low quantity condition is cleared.

Refer to the `threshold monitoring` command for additional information on thresholding.

**Example**
The following command configures the system to support the Alarm thresholding model:

```
threshold model alarm
```
**threshold monitoring**

Enables thresholding for the selected value.

**Product**
All

**Privilege**
Administrator

**Syntax**

```bash
[ no | default ] threshold monitoring { aaa-acct-archive-size | aaa-acct-failure
| aaa-auth-failure | aaa-retry-rate | aaamgr-request-queue | asngw | call-setup
| content-filtering | cpu-resource | cpu-session-throughput | csaf-service |
diameter | ecs | fa-service | firewall | ha-service | hsgw-service | ipsec |
license | lma-service | mme-service | packets-filtered-dropped | packets-forwarded-to-cpu | pdm-service | pgw-service |
route-service | sgw-service | subscriber | system }
```

**no**
Disables threshold monitoring for the specified value.

**default**
Sets / restores default value assigned for the specified parameter.

**aaa-acct-archive-size**
Enables threshold monitoring for the size of the AAA accounting record archive.

**aaa-acct-failure**
Enables threshold monitoring for AAA accounting failures and AAA accounting failure rate values. Refer to the `threshold aaa-acct-failure` and `threshold aaa-acct-failure-rate` commands for additional information on these values.

**aaa-auth-failure**
Enables threshold monitoring for AAA authentication failures and AAA authentication failure rate values. Refer to the `threshold aaa-auth-failure` and `threshold aaa-auth-failure-rate` commands for additional information on these values.

**aaa-retry-rate**
Enables threshold monitoring for the AAA retry rate value. Refer to the `threshold aaa-retry-rate` command for additional information on this value.

**aaamgr-request-queue**
Enables threshold monitoring for AAA Manager Requests for each AAA manager process. Refer to the `threshold aaamgr-request-queue` command for additional information on these values.
asngw
Enables the threshold monitoring for ASN-GW services.

call-setup
Enables threshold monitoring for the call setup, call setup failures, and no-resource rejected call values. Refer to the `threshold call-setup`, `threshold call-setup-failure`, `threshold ppp-setup-fail-rate`, `threshold rp-setup-fail-rate`, and `threshold call-reject-no-resource` commands for additional information on these values.

cpu-resource

cpu-session-throughput
Enables threshold monitoring for the CPU session throughput value. Refer to the `threshold cpu-session-throughput` command for additional information on this value.

content-filtering
Enables threshold monitoring for the Content Filtering service.

cscf-service
Enables threshold monitoring for the CSCF service.

diameter
Enables threshold monitoring for Diameter.

ces
Enables threshold monitoring for the Enhanced Charging Service (ECS).

fa-service
Enables threshold monitoring for Registration Reply errors for each FA service. Refer to the `threshold reg-reply-error` FA Service Configuration Mode command for additional information on this value.

firewall
Enables threshold monitoring for the Stateful Firewall service. Default: Disabled
Refer to the `threshold fw-deny-rule`, `threshold fw-dos-attack`, `threshold fw-drop-packet`, and `threshold fw-no-rule` commands for additional information on this value.
**Important:** Stateful Firewall thresholds can only be enabled if the Stateful Firewall license is present.

**ha-service**
Enables threshold monitoring for Registration Reply errors, re-registration reply errors, deregistration reply errors, and average calls setup per second for each HA service and average calls setup per second at the context level. Refer to the `threshold init-rrq-rcvd-rate`, `threshold reg-reply-error`, `threshold rereg-reply-error`, and `threshold dereg-reply-error` HA Service Configuration Mode commands and the `threshold ha-service init-rrq-rcvd-rate` Context Configuration mode command for additional information on this value.

**hsgw-service**
Enables threshold monitoring for HSGW services. Refer to the `threshold total-hsgw-sessions` for more information on HSGW thresholds.

**ipsec**
Enables monitoring of IPSec thresholds. Refer to the HA-Service Configuration Mode chapter of the Command Line Interface Reference for information on the IPSec thresholds.

**license**
Enables threshold monitoring for the session license value. Refer to the `threshold license` command for additional information on this value.

**lma-service**
Enables threshold monitoring for LMA services. Refer to the `threshold total-lma-sessions` for more information on LMA thresholds.

**mme-service**
Default: Disabled. Enables threshold monitoring for the MME services. Refer to the `threshold total-mme-sessions` commands for additional information on this value.

**packets-filtered-dropped**
Enables threshold monitoring for the filtered/dropped packet value. Refer to the `threshold packets-filtered-dropped` command for additional information on this value.

**packets-forwarded-to-cpu**
Enables threshold monitoring for the forwarded packet value. Refer to the `threshold packets-forwarded-to-cpu` command for additional information on this value.

**pdg-service**
Enables threshold monitoring for PDG service. Threshold monitoring for PDG service is disabled by default.
Enables threshold monitoring for PDIF service.

**pdsn-service**

Enables threshold monitoring for average calls setup per second for contexts and for PDSN services, A11 Request.

Refer to the `threshold packets-forwarded-to-cpu` command for additional information on this value.

**pgw-service**

Enables threshold monitoring for P-GW services.

Refer to the `threshold total-pgw-sessions` for more information on P-GW thresholds.

**route-service**

Enables threshold monitoring for BGP/VRF route services.

Refer to the `ip maximum-routes` command in Context configuration mode and `threshold route-service bgp-routes` in this mode for more information on route thresholds.

**sgw-service**

Enables threshold monitoring for S-GW services.

Refer to the `threshold total-sgw-sessions` for more information on S-GW thresholds.

**subscriber**

Enables threshold monitoring for the subscriber and session values.

Refer to the `threshold subscriber active`, `threshold subscriber total`, `threshold total-ggsn-sessions`, `threshold total-gprs-sessions`, `threshold total-gprs-pdp-sessions`, `threshold total-ha-sessions`, `threshold total-lns-sessions`, `threshold total-pdsn-sessions`, and `threshold per-service-ggsn-sessions`, `threshold per-service-ha-sessions`, `threshold per-service-lns-sessions`, and `threshold per-service-pdsn-sessions` commands for additional information on these values.

**system**

Enables system (chassis) thresholds monitoring.

---

**Usage**

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e., high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.
The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

**Table 24. Thresholding Reporting Mechanisms by Model**

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

In addition to the values that can be enabled by this command, the system supports the enabling of threshold monitoring for IP pool address availability (refer to the `ip pool` and threshold commands in this reference) and port utilization (refer to the threshold commands in this chapter).

**Example**

The following command enables thresholding for subscriber totals:

```bash
threshold monitoring subscriber
```
threshold nat-port-chunks-usage

This command configures the NAT port chunk utilization threshold settings.

**Important:** This command is only available in Release 8.3 and later releases.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
threshold nat-port-chunks-usage high_thresh [ clear low_thresh ]
default threshold nat-port-chunks-usage
```

- **default**
  Configures the default settings.

- **high_thresh**
  Default: 0
  Specifies the high nat-port-chunks-usage threshold that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low nat-port-chunks-usage threshold that must be met within the polling interval for a clear alarm to be generated.
  `low_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the `high_thresh` will be high and low threshold setting.

**Usage**
Use this command to configure the NAT port chunk utilization threshold settings.

**Example**
The following command sets the NAT port chunk utilization threshold settings to a high of 75 and a low of 15:

```plaintext
threshold nat-port-chunks-usage 75 clear 15
```
threshold packets-filtered-dropped

Configures filtered/dropped packet thresholds for the system.

**Product**

PDSN, GGSN, HA, SGSN, ASN GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
threshold packets-filtered-dropped high_thres [ clear low_thres ]
```

1. **high_thres**
   - Default: 0
   - The high threshold number of filtered/dropped packets experienced by the system resulting from ACL rules that must be met or exceeded within the polling interval to generate an alert or alarm.
   - The number can be configured to any integer value between 0 and 1000000000. A value of 0 disables the threshold.

2. **clear low_thres**
   - Default: 0
   - The low threshold number of filtered/dropped packets experienced by the system resulting from ACL rules that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
   - The number can be configured to any integer value between 0 and 1000000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Filtered/dropped packet thresholds generate alerts or alarms based on the total number of packets that were filtered or dropped by the system as a result of access control list (ACL) rules during the specified polling interval.

Alerts or alarms are triggered for filtered/dropped packets based on the following rules:

- **Enter condition:** Actual number of filtered/dropped packets ≥ High Threshold
- **Clear condition:** Actual number of filtered/dropped packets < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value. In addition, refer to information on ACLs in this reference.

**Example**

Refer to the command reference for examples.
The following command configures a filtered/dropped packet high threshold count of 150000 for a system using the Alert thresholding model:

```
threshold packets-filtered-dropped 150000
```
threshold packets-forwarded-to-cpu

Configures forwarded packet thresholds for the system.

Product
PDSN, GGSN, HA, SGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax

\texttt{threshold packets-forwarded-to-cpu high\_thresh \{ clear low\_thresh\}}

\texttt{high\_thresh}
Default: 0
The high threshold number of forwarded packets experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value between 0 and 1000000000. A value of 0 disables the threshold.

\texttt{clear low\_thresh}
Default: 0
The low threshold number of forwarded packets experienced by the system that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 1000000000. A value of 0 disables the threshold.

\textbf{Important:} This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Forwarded packet thresholds generate alerts or alarms based on the total number of packets that were forwarded to active system CPU(s) during the specified polling interval. Packets are forwarded to active system CPUs when the NPUs do not have adequate information to properly route them.

\textbf{Important:} Ping and/or traceroute packets are intentionally forwarded to system CPUs for processing. These packet types are included in the packet count for this threshold.

Alerts or alarms are triggered for forwarded packets based on the following rules:

\begin{itemize}
  \item \textbf{Enter condition:} Actual number of forwarded packets \geq \text{High Threshold}
  \item \textbf{Clear condition:} Actual number of forwarded packets < \text{Low Threshold}
\end{itemize}

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a forwarded packet high threshold count of 10000 for an system using the Alert thresholding model:

```
threshold packets-forwarded-to-cpu 10000
```
threshold pdg-current-active-sessions

Configures the threshold for monitoring the total number of all current PDG sessions only.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Syntax

```
threshold pdg-current-active-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Configures the total number of active PDG sessions to be monitored on a chassis. `high_thresh` is any integer from 0 to 300000.
  There is no default, but 0 means that there is no threshold monitoring.

- **clear low_thresh**
  Clears any percentage of the number of sessions being monitored using the `high_thresh` variable defined above.
  `low_thresh` is any integer from 0 to 300000.

Usage
Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of active PDG sessions for an entire chassis.

Example
The following command configures a monitoring threshold of 300000 active PDG sessions on a chassis:

```
threshold pdg-current-active-sessions 300000
```

which turns out to be too many, so the following command clears 100000:

```
threshold pdg-current-active-sessions 30000 clear 10000
```
threshold pdg-current-sessions

Configures the threshold for monitoring the total number of all current PDG sessions, including inactive sessions.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold pdg-current-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Configures the total number of PDG sessions on a chassis, both active and inactive. `high_thresh` is any integer from 0 to 300000.
  There is no default, but 0 means that there is no threshold monitoring.

- **clear low_thresh**
  Clears any percentage of the number of sessions being monitored using the `high_thresh` variable defined above.
  `low_thresh` is any integer from 0 to 300000.

**Usage**

Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of PDG sessions, both active and inactive, for an entire chassis.

**Example**
The following command configures a monitoring threshold of 300000 active and inactive PDG sessions on a chassis:

```
threshold pdg-current-sessions 300000
```

which turns out to be too many, so the following command clears 100000:

```
threshold pdg-current-sessions 300000 clear 100000
```
threshold pdif-current-sessions

Configures the threshold for monitoring the total number of all current pdif sessions, including inactive sessions.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```bash
threshold pdif-current-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Configures the total number of PDIF sessions on a chassis, both active and inactive. *high_thresh* is any integer from 0 to 300000.
  There is no default, but 0 means that there is no threshold monitoring.

- **clear low_thresh**
  Clears any percentage of the number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is any integer from 0 to 300000.

Usage
Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of PDIF sessions, both active and inactive, for an entire chassis.

Example
The following command configures a monitoring threshold of 300000 active and inactive PDIF sessions on a chassis:

```bash
threshold pdif-current-sessions 300000
```

which turns out to be too many, so the following command clears 100000:

```bash
threshold pdif-current-sessions 300000 clear 100000
```
threshold pdif-current-active-sessions

Configures the threshold for monitoring the total number of current pdif sessions only.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold pdif-current-active sessions high_thres [ clear low_thres ]
```

* high_thres

Configures the total number of active PDIF sessions to be monitored on a chassis. `high_thres` is any integer from 0 to 300000. There is no default, but 0 means that there is no threshold monitoring.

* clear low_thres

Clears any percentage of the number of sessions being monitored using the `high_thres` variable defined above. `low_thres` is any integer from 0 to 300000.

**Usage**
Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of active PDIF sessions for an entire chassis.

**Example**
The following command configures a monitoring threshold of 300000 active PDIF sessions on a chassis:

```
threshold pdif-current-active-sessions 300000
```

which turns out to be too many, so the following command clears 100000:

```
threshold pdif-current-active-sessions 300000 clear 100000
```
threshold per-service-ggsn-sessions

Configures thresholds for the number of PDP contexts per GGSN service in the system.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
threshold per-service-ggsn-sessions high_thresh [clear low_thresh]
```

**high_thresh**
Default: 0
The high threshold number of PDP contexts for any one GGSN service that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of PDP contexts for any one GGSN service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the number of PDP contexts for any GGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:
- **Enter condition:** Actual number of PDP contexts for any GGSN service ≥ High Threshold
- **Clear condition:** Actual number of PDP contexts < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a high threshold count of 10000 subscriber attaches per GGSN service for the Alert thresholding model:
threshold per-service-ggsn-sessions 10000
threshold per-service-gprs-pdp-sessions

Configures thresholds for the number of 2G-activated PDP contexts per GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

threshold per-service-gprs-pdp-sessions high_thresh [ clear low_thresh ]

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The high threshold number of 2G-activated PDP contexts for any one GPRS service. This number must be met or exceeded within the polling interval to generate an alert or alarm. The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The low threshold number of 2G-activated PDP contexts for any one GPRS service. This number or higher maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, then a clear alarm will be generated. The number can be configured to any integer value between 0 and 4000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the number of 2G-activated PDP contexts for any GPRS service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for PDP contexts based on the following rules:
- **Enter condition:** Actual number of PDP contexts for any GPRS service ≥ High Threshold
- **Clear condition:** Actual number of PDP contexts < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll monitoring` command to configure the polling interval and the `threshold poll monitoring` command to enable thresholding for this value.

Example
The following command configures a high threshold count of 10000 2G-activated PDP contexts per GPRS service for the Alert thresholding model:
threshold per-service-gprs-sessions 10000
threshold per-service-gprs-sessions

Configures the thresholds for the number of 2G-attached subscribers per GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold per-service-gprs-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
The high threshold number of 2G-attached subscribers for any one GPRS service. This threshold number must be met or exceeded within the polling interval to generate an alert or alarm. The number can be configured to any integer value from 0 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of 2G-attached subscribers for any one GPRS service. The number of subscribers must remain above this threshold in order to maintain a previously generated alarm condition. If the number of 2G subscribers falls beneath the low threshold within the polling interval, then a clear alarm will be generated. The number can be configured to any integer value between 0 and 2000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the number of 2G-attached subscribers for any GPRS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of 2G-attached subscribers for any GPRS service ≥ High Threshold
- **Clear condition:** Actual number of 2G-attached subscribers < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a high threshold count of 10000 2G-attaches per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```
threshold per-service-ha-sessions

Configures thresholds for the number of HA sessions per HA service in the system.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
threshold per-service-ha-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
The high threshold number of HA sessions for any one HA service that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 500000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
The low threshold number of HA sessions for any one HA service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of HA sessions for any HA service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HA sessions based on the following rules:

- **Enter condition:** Actual number of HA sessions for any HA service \( \geq \) High Threshold
- **Clear condition:** Actual number of HA sessions \(<\) Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a HA session per service high threshold count of 10000 for an system using the Alert thresholding model:
threshold per-service-ha-sessions 10000
threshold per-service-Ins-sessions

Configures thresholds for the number of LNS sessions per LNS service in the system.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

```
threshold per-service-Ins-sessions high_thresh [ clear low_thresh]
```

**high_thresh**
Default: 0
The high threshold number of LNS sessions for any one LNS service that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 500000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of LNS sessions for any one LNS service that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the number of LNS sessions for any LNS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for LNS sessions based on the following rules:
- **Enter condition:** Actual number of LNS sessions for any LNS service \( \geq \) High Threshold
- **Clear condition:** Actual number of LNS sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example
The following command configures a LNS session per service high threshold count of 10000 for an system using the Alert thresholding model:
threshold per-service-1ns-sessions 10000
threshold per-service-pdsn-sessions

Configures thresholds for the number of PDSN sessions per PDSN service in the system.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
threshold per-service-pdsn-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
The high threshold number of PDSN sessions for any one PDSN service that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 500000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of PDSN sessions for any one PDSN service that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the number of PDSN sessions for any PDSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition:** Actual number of PDSN sessions for any PDSN service ≥ High Threshold
- **Clear condition:** Actual number of PDSN sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a HA session per service high threshold count of 10000 for an system using the Alert thresholding model:
threshold per-service-pdsn-sessions 10000
Global Configuration Mode Commands

threshold per-service-sgsn-pdp-sessions

Configures the thresholds for the number of 3G-activated PDP contexts per SGSN service on the system.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

threshold per-service-sgsn-pdp-sessions high_thresh [ clear low_thresh ]

**high_thresh**
Default: 0
The high threshold number of 3G-activated PDP contexts for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of 3G-activated PDP contexts for any one SGSN service. This number or higher maintains a previously generated alarm condition. If the number of 3G-activated PDP contexts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 2400000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the number of 3G-activated PDP contexts for any SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:
- **Enter condition:** Actual number of 3G-activated PDP contexts for any SGSN service ≥ High Threshold
- **Clear condition:** Actual number of 3G-activated PDP contexts < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example
The following command configures a high threshold count of 10000 3G-activated PDP contexts per SGSN service for the system’s Alert thresholding model:
threshold per-service-sgsn-sessions 10000
threshold per-service-sgsn-sessions

Configures the thresholds for the number of 3G-attached subscribers per SGSN service in the system.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
threshold per-service-sgsn-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
The high threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
The low threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 2000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the number of 3G-attached subscribers for any one SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of 3G-attached subscribers for any single SGSN service ≥ High Threshold
- **Clear condition:** Actual number of 3G-attached subscribers for any single SGSN service < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a high threshold count of 10000 3G-attached subscribers per SGSN service for a system using the Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```
**threshold poll**

This command configures the polling interval over which to count or measure the thresholding value.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
```

**default**

Restores the specified parameter to its default value.
**10sec-cpu-utilization percent**
Default: 300 seconds (5 minutes)
Configures the polling interval for measuring a 10 second average of CPU utilization.

---

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

---

**all-rrp-failure**
Default: 0
Configures the polling interval over which to count A11 Registration Response failures. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

---

**all-rrq-msg-discard**
Default: 0
Configures the polling interval over which to count how many A11 Registration Request messages are discarded. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

---

**all-rac-msg-discard**
Default: 0
Configures the polling interval over which to count how many A11 Registration Acknowledgement messages are discarded. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

---

**aaa-acct-archive-size**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count archived AAA accounting messages.

---

**aaa-acct-failure**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count failed AAA accounting requests.

---

**aaa-acct-failure-rate**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of AAA accounting failures.

---

**aaa-auth-failure**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count failed authentication requests.

---

**aaa-auth-failure-rate**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of AAA authentication failures.

---

**aaa-retry-rate**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percent of AAA request message retries.

### aaamgr-request-queue
Default: 0
Configures the polling interval over which to count the number AA Manager Requests for each AAA manager process. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

### active-subscriber
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of active subscriber sessions.

### all-ppp-send-discard
Default: 0
Configures the polling interval over which to count the number of discarded PPP send packets. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

### available-ip-pool-group
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure IP pool utilization.

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

### call-reject-no-resource
Default: 900 seconds (15 minutes)
Configures the polling interval over which to count the number of calls rejected due to insufficient resources.

### call-setup
Default: 900 seconds (15 minutes)
Configures the polling interval over which to count the number of calls setup.

### call-setup-failure
Default: 900 seconds (15 minutes)
Configures the polling interval over which to count the number of calls setup failures.

### call-setup-failures
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF call setup failures. `time` must be an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

### call-total-active
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF total active calls.
$time$ must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**cpu-available-memory**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure PSC/PSC2 CPU memory availability.

**Important:** When specifying $interval$ $time$ for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**Important:** This command is not supported on all platforms

**cpu-load**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure PSC/PSC2 CPU load using a 5 minute average measurement.

**Important:** When specifying $interval$ $time$ for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**Important:** This command is not supported on all platforms

**cpu-memory-usage**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of total PSC/PSC2 CPU memory used.

**Important:** When specifying $interval$ $time$ for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**Important:** This command is not supported on all platforms

**cpu-orbs-crit**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for critical-level alerts.

**cpu-orbs-warn**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for warning-level alerts.
**threshold poll**

*Global Configuration Mode Commands*

**cpu-session-throughput**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure PSC/PSC2 CPU session throughput.

**Important:** This command is not supported on all platforms

**cpu-utilization**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure PSC/PSC2 CPU utilization.

**Important:** When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**Important:** This command is not supported on all platforms

**cscf-invite-rcvd**
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count the CSCF calls. time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**cscf-reg-rcvd**
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count the CSCF registrations. time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**cscf-service-route-failures**
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count the CSCF service route failures. time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**dcca-bad-answers**
Configures the polling interval in seconds over which to count Diameter bad answers.

**dcca-protocol-error**
Configures the polling interval in seconds over which to count Diameter protocol errors.

**dcca-rating-failed**
Configures the polling interval in seconds over which to count Diameter rating failures.
**dcca-unknown-rating-group**
Configures the polling interval in seconds over which to count Diameter unknown rating group errors.

**dereg-reply-error**
Default: 0
Configures the polling interval over which to measure the number of de-registration reply errors for HA services. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

**edr-file-space**
Configures the polling interval in seconds over which to count EDR file space.

**edr-udr-dropped-flow-control**
Configures the polling interval in seconds over which to count EDR-UDRs Dropped due to Flow Control at ACSMGR.

**error-no-resource**
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF No Resource Errors.

*time* must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**error-presence**
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF Presence Errors.

*time* must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**error-reg-auth**
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF Reg-Auth Errors.

*time* must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**error-tcp**
Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF TCP Errors.

*time* must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

**fa-reg-reply-error**
Default: 0
Configures the polling interval over which to measure the number of registration reply errors for FA services. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

**fng-current-active-sessions**
Configures the polling interval in seconds over which to count FNG current active sessions.
### Global Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fng-current-sessions</strong></td>
<td>Configures the polling interval in seconds over which to count FNG current sessions.</td>
</tr>
<tr>
<td><strong>fw-deny-rule</strong></td>
<td>Default: 900 seconds (15 minutes) Configures the Stateful Firewall Deny-Rule threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.</td>
</tr>
<tr>
<td><strong>fw-dos-attack</strong></td>
<td>Default: 900 seconds (15 minutes) Configures the Stateful Firewall DoS-Attacks threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.</td>
</tr>
<tr>
<td><strong>fw-drop-packet</strong></td>
<td>Default: 900 seconds (15 minutes) Configures the Stateful Firewall Drop-Packet threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.</td>
</tr>
<tr>
<td><strong>fw-no-rule</strong></td>
<td>Default: 900 seconds (15 minutes) Configures the Stateful Firewall No-Rule threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.</td>
</tr>
<tr>
<td><strong>ha-init-rrq-rcvd-rate</strong></td>
<td>Configures the polling interval over which to measure the average number of calls setup per minute for the context. When specifying <code>interval time</code> for this threshold, the range is from 60 through 900 seconds.</td>
</tr>
<tr>
<td><strong>ha-svc-init-rrq-rcvd-rate</strong></td>
<td>Configures the polling interval over which to measure the average number of calls setup per minute for HA services. When specifying <code>interval time</code> for this threshold, the range is from 60 through 900 seconds.</td>
</tr>
<tr>
<td><strong>ip-pool-free</strong></td>
<td>Default: 300 seconds (5 minutes) Configures the polling interval over which to measure the percentage of the IP pool addresses that are in the free state.</td>
</tr>
</tbody>
</table>

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.) |

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-pool-hold</strong></td>
<td>Default: 300 seconds (5 minutes) Configures the polling interval over which to measure the percentage of the IP pool address that are in the hold state.</td>
</tr>
</tbody>
</table>
Global Configuration Mode Commands

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

### ip-pool-release
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of IP pool address that are in the release state.

### ip-pool-used
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of the IP pool addresses that are used.

### ipsec-ipsec-call-req-rej
Default: 900
Configures the polling interval over which to count the IPSec call requests that are rejected.

### ipsec-ike-failrate
Default: 900
Configures the polling interval over which to count the IPSec IKE failure rate.

### ipsec-ike-failures
Default: 900
Configures the polling interval over which to count the IPSec IKE failures.

### ipsec-ike-requests
Default: 900
Configures the polling interval over which to count the IPSec IKE request.

### ipsec-tunnels-established
Default: 900
Configures the polling interval over which to count the IPSec tunnels established.

### ipsec-tunnels-setup
Default: 900
Configures the polling interval over which to count the IPSec tunnels setup.
**license-remaining-session**
Default: 900 seconds (15 minutes)
Configures the polling interval over which to measure session license utilization.

**mgmt-cpu-memory-usage interval**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure SMC CPU memory usage.

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**Important:** This command is not supported on all platforms.

**mgmt-cpu-utilization**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure SMC CPU usage.

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**Important:** This command is not supported on all platforms.

**nat-port-chunks-usage**

**Important:** This keyword is only available in Release 8.3 and later.

Default: 900 seconds (15 minutes)
Configures the polling interval over which to measure NAT port chunks usage.

**packets-filtered-dropped**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the filtered/dropped packets.

**packets-forwarded-to-cpu**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the forwarded packets.

**pdg-current-active-sessions**
Configures how frequently the system polls the pdg-current-active-sessions threshold.
**Threshold Poll**

### pdg-current-sessions

Configures how frequently the system polls the pdg-current-sessions threshold.

#### threshold poll pdif-current-sessions interval period

Configures the polling interval for all current PDIF sessions in seconds rounded to the nearest multiple of 30 seconds. `period` is any integer from 30 to 60000.

#### threshold poll pdif-current-active-sessions interval period

Configures the polling interval for active sessions only in seconds rounded to the nearest multiple of 30 seconds. `period` is any integer from 30 to 60000.

### psdn-init-rrq-rcvd-rate

Default: 0

Configures the polling interval over which to measure the average number of calls setup per second for a PDSN-service. When specifying `interval time` for this threshold, the range is from 60 through 900 seconds.

### psdn-svc-init-rrq-rcvd-rate

Configures the polling interval in seconds over which to count PDSN per-service call received rate.

### per-service-asngw-sessions

Configures the polling interval in seconds over which to count per service ASNGW sessions.

### per-service-ggsn-sessions

Default: 300 seconds (5 minutes)

Configures the polling interval over which to count the number of PDP contexts per GGSN service.

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

### per-service-gprs-sessions

Default: 300 seconds (5 minutes)

Configures the polling interval during which the SGSN counts the number of 2G-attached subscriber per GPRS service.

**Important:** When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

### per-service-gprs-pdp-sessions

Default: 300 seconds (5 minutes)

Configures the polling interval during which the SGSN counts the number of 2G-activated PDP contexts per GPRS service.
<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>threshold poll</code></td>
<td></td>
<td>Configures the polling interval over which to count the number of HA sessions per HA service.</td>
</tr>
<tr>
<td><strong>Important</strong>: When specifying <code>interval</code> for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>per-service-ha-sessions</code></td>
<td>Default: 300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the number of HA sessions per HA service.</td>
</tr>
<tr>
<td><strong>Important</strong>: When specifying <code>interval</code> for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>per-service-lns-sessions</code></td>
<td>Default: 300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the number of LNS sessions per LNS service.</td>
</tr>
<tr>
<td><strong>Important</strong>: When specifying <code>interval</code> for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>per-service-pdsn-sessions</code></td>
<td>Default: 300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the number of PDSN sessions per PDSN service.</td>
</tr>
<tr>
<td><strong>Important</strong>: When specifying <code>interval</code> for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>per-service-sgsn-sessions</code></td>
<td>Default: 300 seconds (5 minutes)</td>
<td>Configures the polling interval during which the SGSN counts the number of 3G-attached subscribers per SGSN service.</td>
</tr>
<tr>
<td><strong>Important</strong>: When specifying <code>interval</code> for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>per-service-sgsn-pdp-sessions</code></td>
<td>Default: 300 seconds (5 minutes)</td>
<td>Configures the polling interval during which the SGSN counts the number of 3G-activated PDP contexts per SGSN service.</td>
</tr>
</tbody>
</table>
### Important:
When specifying `interval time` for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port-high-activity</code></td>
<td>300 seconds</td>
<td>Configures the polling interval over which to measure high port activity.</td>
</tr>
<tr>
<td><code>port-rx-utilization</code></td>
<td>300 seconds</td>
<td>Configures the polling interval over which to measure receive port utilization.</td>
</tr>
<tr>
<td><code>port-tx-utilization</code></td>
<td>300 seconds</td>
<td>Configures the polling interval over which to measure transmit port utilization.</td>
</tr>
<tr>
<td><code>ppp-setup-fail-rate</code></td>
<td>900 seconds</td>
<td>Configures the polling interval over which to measure the PPP setup failure rate.</td>
</tr>
<tr>
<td><code>reg-reply-error</code></td>
<td>0</td>
<td>Configures the polling interval over which to measure number of registration reply errors for HA services. When specifying <code>interval time</code> for this threshold, the range is from 60 through 900 seconds.</td>
</tr>
<tr>
<td><code>reg-total-active</code></td>
<td>300 seconds</td>
<td>Configures the polling interval over which to measure CSCF Total Active Registrations. <code>time</code> must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.</td>
</tr>
<tr>
<td><code>rereg-reply-error</code></td>
<td>0</td>
<td>Configures the polling interval over which to measure number of re-registration reply errors for HA services. When specifying <code>interval time</code> for this threshold, the range is from 60 through 900 seconds.</td>
</tr>
</tbody>
</table>
rp-setup-fail-rate
Default: 900 seconds (15 minutes)
Configure the polling interval over which to measure the RP setup failure rate.

spc-cpu-memory-usage interval

Important: This command has been renamed to threshold mgmt-cpu-memory-usage. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

Important: This command is not supported on all platforms

spc-cpu-utilization

Important: This command has been renamed to threshold mgmt-cpu-utilization. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

Important: This command is not supported on all platforms

storage-utilization
Default: 900 seconds (15 minutes)
Configures the polling interval over which to record the CompactFlash utilization percentage threshold interval in seconds.

total-asngw-sessions
Configures the polling interval over which to measure total ASNGW sessions on the system.

total-ggsn-sessions
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of GGSN sessions on the system.

Important: When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-gprs-sessions
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of 2G-attached subscribers on the system.

Important: When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)
**total-gprs-pdp-sessions**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of 2G-activated PDP contexts per GPRS sessions on the system.

**Important:** When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**total-ha-sessions**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of HA sessions on the system.

**Important:** When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**total-hsgw-sessions**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of HSGW sessions on the system.

**Important:** When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**total-lma-sessions**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of LMA sessions on the system.

**Important:** When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**total-lns-sessions**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of LNS sessions on the system.

**Important:** When specifying interval time for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

**total-pdsn-sessions**
Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of PDSN sessions on the system.
<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>total-pgw-sessions</strong></td>
<td>300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the total number of P-GW sessions on the system.</td>
</tr>
<tr>
<td><strong>total-sgsn-sessions</strong></td>
<td>300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the total number of SGSN sessions on the system.</td>
</tr>
<tr>
<td><strong>total-sgsn-pdp-sessions</strong></td>
<td>300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the total number of SGSN sessions on the system.</td>
</tr>
<tr>
<td><strong>total-sgw-sessions</strong></td>
<td>300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the total number of S-GW sessions on the system.</td>
</tr>
<tr>
<td><strong>total-subscriber</strong></td>
<td>300 seconds (5 minutes)</td>
<td>Configures the polling interval over which to count the total number of subscriber sessions.</td>
</tr>
</tbody>
</table>

**Important:** When specifying *interval time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

*interval* time

Specifies the amount of time that comprises the polling interval. *time* is measured in seconds and can be configured to any integer value from 60 to 60000 unless otherwise noted in keyword descriptions.
Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.

Example

The following command configures the polling interval for the total subscribers threshold value to 600 seconds (10 minutes):

```
threshold poll total-subscriber interval 600
```
threshold poll asngw-auth-failure

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway authentication failure.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll asngw-auth-failure interval dur
```

```
default threshold poll asngw-auth-failure interval
```

```
default
Restores the specified parameter to its default value 300 seconds.
```

```
interval dur
Default: 300 seconds.
Specifies the amount of time that comprises the polling interval.
dur is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.
```

**Usage**
This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval to 600 seconds for the ASN Gateway authentication failure threshold:

```
threshold poll asngw-auth-failure interval 600
```
threshold poll asngw-handoff-denial

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway hand-off denial.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll asngw-handoff-denial interval \( \text{dur} \)
default threshold poll asngw-handoff-denial interval
```

**Default**
Restores the specified parameter to its default value 300 seconds.

**interval \( \text{dur} \)**
Default: 300 seconds.
Specifies the polling interval time.
\( \text{dur} \) is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.

**Usage**
This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval to 600 seconds for hand-off denial threshold:

```
threshold poll asngw-handoff-denial interval 600
```
threshold poll asngw-max-eap-retry

Configures the polling interval over which to count or measure the thresholding value for maximum EAP authentication retries.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
threshold poll asngw-max-eap-retry interval dur
```

```
default threshold poll asngw-max-eap-retry interval
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restores the specified parameter to its default value 300 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval dur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 300 seconds.</td>
</tr>
<tr>
<td>Specifies the amount of time that comprises the polling interval.</td>
</tr>
<tr>
<td>dur is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.</td>
</tr>
</tbody>
</table>

**Usage**

This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**

The following command configures the polling interval to 600 seconds for maximum EAP authentication retry threshold:

```
threshold poll asngw-max-eap-retry interval 600
```
threshold poll asngw-network-entry-denial

Configures the polling interval over which to count or measure the thresholding value for network entry denial to an MS.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

threshold poll asngw-network-entry-denial interval \textit{dur}

default threshold poll asngw-network-entry-denial interval

default
Restores the specified parameter to its default value 300 seconds.

\textbf{interval} \textit{dur}
Default: 300 seconds.
Specifies the amount of time that comprises the polling interval.
\textit{dur} is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.

Usage
This command dictates the time period over which to monitor the specified value for threshold crossing.

\textbf{Important:} All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the \textbf{threshold monitoring} and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Example
The following command configures the polling interval to 600 seconds for network entry denial threshold:

\texttt{threshold poll asngw-network-entry-denial interval 600}
threshold poll asngw-r6-invalid-nai

Configures the polling interval over which to count or measure the thresholding value for invalid NAIs in R6 messages.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

threshold poll asngw-r6-invalid-nai interval \textit{dur}

default threshold poll asngw-r6-invalid-nai interval

default
Restores the specified parameter to its default value 300 seconds.

interval \textit{dur}
Default: 300 seconds.
Specifies the amount of time that comprises the polling interval.
\textit{dur} is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.

Usage
This command dictates the time period over which to monitor the specified value for threshold crossing.

\textbf{Important:} All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the \textit{threshold monitoring} and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Example
The following command configures the polling interval to \textit{600} seconds for invalid NAIs in R6 messages threshold:

\texttt{threshold poll asngw-r6-invalid-nai interval 600}
threshold poll asngw-session-setup-timeout

Configures the polling interval over which to count or measure the thresholding value for session setup timeout.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
threshold poll asngw-session-setup-timeout interval \( \text{dur} \)
```

default threshold poll asngw-session-setup-timeout interval

- **default**
  Restores the specified parameter to its default value 300 seconds.

- **interval \( \text{dur} \)**
  Default: 300 seconds.
  Specifies the amount of time that comprises the polling interval.
  \( \text{dur} \) is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.

**Usage**
This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval to 600 seconds for session setup timeout threshold:

```plaintext
threshold poll asngw-session-setup-timeout interval 600
```
threshold poll asngw-session-timeout

Configures the polling interval over which to count or measure the thresholding value for session timeout.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll asngw-session-timeout interval dur
```

```
default threshold poll asngw-session-timeout interval
```

**default**
Restores the specified parameter to its default value 300 seconds.

**interval**  `dur`
Default: 300 seconds.
Specifies the amount of time that comprises the polling interval.
`dur` is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.

**Usage**
This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval to 600 seconds for session timeout threshold:

```
threshold poll asngw-session-timeout interval 600
```
threshold poll cdr-file-space

This command configures the polling interval for CDR File Space Usage threshold.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

threshold poll cdr-file-space interval duration

default threshold poll cdr-file-space interval

default
- Configures the default setting.
- Default: 300 seconds.

interval duration
- Specifies the polling interval for CDR File Space Usage threshold, in seconds.
- duration must be an integer value from 60 through 60000.

Usage
This command configures the polling interval for CDR File Space Usage threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Example
The following command configures the polling interval to 600 seconds for the CDR file space usage threshold:

    threshold poll cdr-file-space interval 600
threshold poll contfilt-block

This command configures the polling interval Content Filtering Block threshold.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll contfilt-block interval duration

default threshold poll contfilt-block
```

**Usage**
This command configures the polling interval Content Filtering Block threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval to **600 seconds** for the content filtering blocking threshold:

```
threshold poll contfilt-block interval 600
```
threshold poll contfilt-rating

This command configures the polling interval for the Content Filtering Rating threshold.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll contfilt-rating interval duration
default threshold poll contfilt-rating
```

default
Configures the default setting.
Default: 300 seconds.

```
interval dur
```
Specifies the polling interval for the Content Filtering Rating threshold, in seconds.
`duration` must be an integer value from 60 through 60000.

**Usage**
This command configures the polling interval for the Content Filtering Rating threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval to 600 seconds for the content filtering rating processing threshold:

```
threshold poll contfilt-rating interval 600
```
threshold poll dcca-protocol-error

This command configures the polling interval for DCCA Protocol Error threshold.

**Product**
- ECS

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
threshold poll dcca-protocol-error interval duration

default threshold poll dcca-protocol-error interval
```

**default**
- Configures the default setting.
- Default: 900 seconds

**interval duration**
- Specifies the polling interval for DCCA Protocol Error threshold, in seconds.
- `duration` must be an integer value from 60 through 60000.

**Usage**
- Use this the polling interval for DCCA Protocol Error threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholding in this chapter.

**Example**
- The following command configures the polling interval to 600 seconds for the DCCA protocol error threshold:

```
threshold poll dcca-protocol-error interval 600
```
threshold poll dcca-rating-failed

This command configures the polling interval for DCCA Rating Failed threshold.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
threshold poll dcca-rating-failed interval duration
```

default threshold poll dcca-rating-failed interval

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the default setting.</td>
</tr>
<tr>
<td>Default: 900 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the polling interval for DCCA Rating Failed threshold.</td>
</tr>
<tr>
<td>duration must be an integer value from 60 through 60000.</td>
</tr>
</tbody>
</table>

Usage
This command configures the polling interval for DCCA Rating Failed threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholding in this chapter.

Example
The following command configures the polling interval to 600 seconds for the Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject thresholds:

```
threshold poll dcca-rating-failed interval 600
```
threshold poll dcca-bad-answers

This command configures the polling interval for DCCA Bad Answers threshold—invalid or bad response to the system from the Diameter server.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll dcca-bad-answers interval duration
```

default threshold poll dcca-bad-answers interval

default
Configures the default setting.
Default: 900 seconds

```
interval duration
```

Specifies the polling interval for DCCA Bad Answers threshold, in seconds.
`duration` must be an integer value from 60 through 60000.

**Usage**
This command configures the polling interval for DCCA Bad Answers threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholding in this chapter.

**Example**
The following command configures the polling interval to 600 seconds for invalid or bad response threshold to the system from Diameter server:

```
threshold poll dcca-rating-failed interval 600
```
threshold poll dcca-unknown-rating-group

This command configures the polling interval for DCCA Unknown Rating Group threshold.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll dcca-unknown-rating-group interval duration
default threshold poll dcca-unknown-rating-group interval
```

**Usage**
This command configures the polling interval for DCCA Unknown Rating Group threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholding in this chapter.

**Example**
The following command configures the polling interval to 600 seconds to threshold for the unknown DCCA Rating Group (content-id) returned by Diameter to system:

```
threshold poll dcca-unknown-rating-group interval 600
```
threshold poll diameter-retry-rate

This command configures the polling interval for Diameter Retry Rate threshold.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

- `threshold poll diameter-retry-rate interval duration`
- `default threshold poll diameter-retry-rate interval`

**default**

Configures the default setting.
Default: 300 seconds

**interval duration**

Specifies the polling interval for Diameter Retry Rate threshold, in seconds.
`duration` must be an integer from 60 through 60000. The input will be rounded up to the closest multiple of 30.

Usage

This command specifies the polling interval for Diameter Retry Rate threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands in this chapter for additional information on the system’s support for thresholding.

Example

The following command configures the Diameter Retry Rate threshold polling interval to 600 seconds:

```
threshold poll diameter-retry-rate interval 600
```
threshold poll edr-file-space

This command configures the polling interval for EDR File Space Usage threshold.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

threshold poll edr-file-space interval duration

interval duration
Default: 300 seconds.
Specifies the polling interval for EDR File Space Usage threshold, in seconds.
duration must be an integer value from 60 through 60000.

Usage
This command configures the polling interval for EDR File Space Usage threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling
interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring ecs and other threshold commands for additional information on
the system’s support for thresholds in this chapter.

Example
The following command configures the polling interval to 600 seconds for the EDR file space usage threshold:

threshold poll edr-file-space interval 600
threshold poll mme-attach-failure

This command configures the polling interval to count the MME Attach Failure messages across all MME services in the system.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll mme-attach-failure interval <dur>
default threshold poll mme-attach-failure interval
```

**default**
Restores the poll interval value to its default value of 900 seconds.

**interval <dur>**
Default: 900 seconds.
Specifies the amount of time that comprises the polling interval for threshold to count the MME Attach Failure messages across all MME services in the system.
<dur> is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.

**Usage**
Use this command to configure the polling interval to count the MME Attach Failure messages across all MME services in the system to generate threshold value.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring mme-service` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval of 600 seconds to count the MME Attach Failure messages for threshold limit:

```
threshold poll mme-attach-failure interval 600
```
threshold poll mme-auth-failure

This command configures the polling interval to count the MME Authentication Failure messages across all MME services in the system.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold poll mme-auth-failure interval <dur>
default threshold poll mme-auth-failure interval
```

**default**
Restores the specified poll interval value to its default value of 900 seconds.

**interval <dur>**
Default: 900 seconds.
Specifies the amount of time that comprises the polling interval for threshold to count the MME Authentication Failure messages across all MME services in the system.
<dur> is measured in seconds and can be configured to any integer value from 30 to 60000 in multiple of 30.

**Usage**
Use this command to configure the polling interval to count the MME Auth Failure messages across all MME services in the system to generate threshold value.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring mme-service` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**
The following command configures the polling interval of 600 seconds to count the MME Auth Failure messages for threshold limit:

```
threshold poll mme-auth-failure interval 600
```
threshold poll total-mme-sessions

This command configures the polling interval over which to count or measure the thresholding value for MME sessions on the system.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ default ] threshold poll total-mme-sessions interval time
```

- **default**
  Restores the threshold poll interval value to its default value of 300 seconds.

- **interval time**
  Default: 900 seconds
  Specifies the amount of time that comprises the polling interval over which to count the total number of MME sessions on the system.
  `time` is measured in seconds and can be configured to any integer value from 30 to 60000.

Usage
This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important**: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

Example
The following command configures the polling interval for the total MME session threshold polling duration value to 600 seconds (10 minutes):

```
threshold poll total-mme-sessions interval 600
```
threshold poll port-rx-utilization

Enables the generation of alerts or alarms based on the port utilization percentage for data received during the polling interval.

Product
All

Privilege
Administrator Security Administrator

Syntax

```
threshold poll port-rx-utilization interval seconds
```

- **interval seconds**
  Configures the threshold polling interval in multiples of 30 seconds from 30 to 60000

Usage

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis configured using the port `port-type slot#/port#` command syntax.

**Important:** This command is not available on all platforms

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Example

Use the following example to configure a threshold poll interval of 300 seconds (5 minutes)

```
threshold poll port-rx-utilization interval 300
```
threshold poll port-tx-utilization

Enables the generation of alerts or alarms based on the port utilization percentage for data transmitted during the polling interval.

**Product**
All

**Privilege**
Administrator Security Administrator

**Syntax**

```
threshold poll port-tx-utilization interval seconds
```

**Usage**
Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis configured using the port `port-type slot#/port#` command syntax.

**Important:** This command is not available on all platforms

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

**Example**
Use the following example to configure a threshold poll interval of 300 seconds (5 minutes)

```
threshold poll port-tx-utilization interval 300
```
**threshold poll port-high-activity**

Enables the generation of alerts or alarms based on the overall port utilization percentage during the polling interval.

**Product**
All

**Privilege**
Administrator Security Administrator

**Syntax**

```
threshold poll port-high-activity interval seconds
```

**Usage**

High port activity thresholds generate alerts or alarms based on the peak utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:

- Enter condition: Actual percent peak utilization of a port ≥ High Threshold
- Clear condition: Actual percent peak utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. This threshold is configured on a per-port basis configured using the `port-type slot#/port#` command syntax.

**Important:** This command is not available on all platforms

**Example**

Use the following example to configure the polling interval over which to measure for high port activity to 300 seconds:

```
threshold poll port-high-activity interval 300
```
threshold poll route-service

This command configures the polling interval over which to count or measure the thresholding value for route services on the system.

**Product**
All

**Privilege**
Administrator Security Administrator

**Syntax**

```
[ default ] threshold poll route-service interval dur
```

- **default**
  Restores the threshold poll interval value to its default value of 900 seconds.

- **interval time**
  Default: 900 seconds
  Specifies the amount of time that comprises the polling interval over which to count the total number of BGP route on the system.
  `dur` is measured in seconds and can be configured to any integer value from 30 to 60000.

**Usage**

This command dictates the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Example**
The following command configures the polling interval for the total BGP routes threshold polling duration value to 600 seconds (10 minutes):

```
threshold poll route-service interval 600
```
threshold ppp-setup-fail-rate

Configures PPP setup failure rate thresholds.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold ppp-setup-fail-rate high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  The high threshold rate for PPP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  `high_thresh` can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Default: 0
  
  The low threshold rate for PPP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  `low_thresh` can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

PPP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of PPP setup failures divided by the total number of PPP sessions initiated. Alerts or alarms are triggered for PPP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures ≥ High Threshold
- **Clear condition:** Actual number of call setup failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a PPP setup failure rate high threshold of 50 and a clear threshold of 45:
threshold ppp-setup-fail-rate 50 clear 45
threshold route-service bgp-routes

This command configures the threshold limits for route services to BGP routes.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold route-service bgp-routes high_thresh [ clear low_thresh ]
```

*high_thresh*

Default: 0

The high threshold rate for BGP routes on the system that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

*clear low_thresh*

Default: 0

The low threshold rate for BGP routes on the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to configure a threshold in percentage of maximum BGP routes allowed. If the percentage of the number of BGP routes in a context (including all VRFs) reaches *high_thresh*, a notification is generated. Optionally, if the threshold subsystem is configured in ‘alarm’ mode, a Threshold_Clear notification is generated when the percentage of the number of BGP routes in a context (including all VRFs) goes below *low_thresh*. The maximum number of BGP routes is also sent by BGP task when getting the stats.

Alerts or alarms are triggered for BGP routes based on the following rules:

- **Enter condition:** Actual number of call setup failures > High Threshold
- **Clear condition:** Actual number of call setup failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example
The following command configures system for high threshold of 50 and a clear threshold of 45:

```
threshold route-service bgp-routes 50 clear 45
```
threshold rp-setup-fail-rate

Configures RP setup failure rate thresholds.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold rp-setup-fail-rate high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
The high threshold rate for RP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
The low threshold rate for RP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
RP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of Registration Request Messages rejected divided by the total number of Registration Request Messages received.

Alerts or alarms are triggered for RP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures ≥ High Threshold
- **Clear condition:** Actual number of call setup failures < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a RP setup failure rate high threshold of 50 and a clear threshold of 45:

```
threshold rp-setup-fail-rate 50 clear 45
```
threshold rp-setup-fail-rate

threshold rp-setup-fail-rate 50 clear 45
threshold spc-cpu-memory-usage

This command has been renamed to threshold mgmt-cpu-memory-usage. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

**Important:** This command is not supported on all platforms.
threshold spc-cpu-utilization

This command has been renamed to `threshold mgmt-cpu-utilization`. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.
**threshold storage-utilization**

Configures SMC CompactFlash memory utilization thresholds.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold storage-utilization high_thresh[ clear low_thresh]
```

- **high_thresh**
  
  Default: 90
  
  The high threshold memory utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  The number can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Default: 90
  
  The low threshold memory utilization percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  The number can be configured to any integer value between 0 and 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

CompactFlash memory utilization thresholds generate alerts or alarms based on the utilization percentage of the CompactFlash on each installed SMC during the specified polling interval. Although, a single threshold is configured for both SMCs, separate alerts or alarms can be generated for each.

Alerts or alarms are triggered for CompactFlash memory utilization based on the following rules:

- **Enter condition:** Actual percentage memory utilization $\geq$ High Threshold
- **Clear condition:** Actual percentage memory utilization $< Low Threshold$

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold CompactFlash utilization percentage of 85 for an system using the Alert thresholding model:
threshold storage-utilization
threshold subscriber active

Configures active subscriber thresholds for the system.

Product
PDSN, GGSN, SGSN, HA

Privilege
Security Administrator, Administrator

Syntax
threshold subscriber active high_thresh [ clear low_thresh ]

high_thresh
Default: 0
The high threshold number of active subscriber sessions facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm. The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
The low threshold number of active subscriber sessions facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated. The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Active subscriber thresholds generate alerts or alarms based on the total number of active subscriber sessions facilitated by the system during the specified polling interval. Alerts or alarms are triggered for active subscriber totals based on the following rules:
● Enter condition: Actual total number of active subscriber sessions ≥ High Threshold
● Clear condition: Actual total number of active subscriber sessions < Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures an active subscriber high threshold count of 150000 and a low threshold of 1500 for an system using the Alarm thresholding model:
threshold subscriber active 150000 clear 1500
threshold subscriber total

Configures total subscriber thresholds for the system.

Product
PDSN, GGSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
threshold subscriber total high_thresh [ clear low_thresh ]
```

---

**high_thresh**

Default: 0

The high threshold number of subscriber sessions (active and dormant) facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

---

**clear low_thresh**

Default: 0

The low threshold number of subscriber sessions (active and dormant) facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

The number can be configured to any integer value between 0 and 100000. A value of 0 disables the threshold.

---

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

---

**Usage**

Total subscriber thresholds generate alerts or alarms based on the total number of subscriber sessions (active and dormant) facilitated by the system during the specified polling interval.

Alerts or alarms are triggered for subscriber totals based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions ≥ High Threshold
- **Clear condition:** Actual total number of subscriber sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

---

**Example**

The following command configures an active subscriber high threshold count of 450000 and a low threshold of 250000 for an system using the Alarm thresholding model:
threshold subscriber total 450000 clear 250000
threshold total-ggsn-sessions

Configures thresholds for the total number of GGSN sessions across all the services in the system.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold total-ggsn-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 0 (Disabled)
  The high threshold number of total GGSN sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.
  The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0 (Disabled)
  The low threshold number of total GGSN sessions that maintains a previously generated alarm condition. If the number of GGSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  The number can be configured to any integer value between 0 and 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the total number of GGSN sessions across all the services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of GGSN sessions based on the following rules:
- **Enter condition:** Actual total number of GGSN sessions ≥ High Threshold
- **Clear condition:** Actual total number of GGSN sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a total GGSN session high threshold count of 10000 for an system using the Alert thresholding model:
threshold total-ggsn-sessions

threshold total-ggsn-sessions 10000
threshold total-gprs-sessions

Configures thresholds for the total number of GPRS sessions in the system.

Product
SGSN

Privilege
Administrator

Syntax

```
threshold total-gprs-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
The high threshold number of total GPRS sessions for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 1 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of total GPRS sessions for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 200000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:
- **Enter condition:** Actual total number of GPRS sessions ≥ High Threshold
- **Clear condition:** Actual total number of GPRS sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

**Example**
The following command configures a total number of GPRS sessions high threshold count of 10000 for a system using the Alert thresholding model:
threshold total-gprs-sessions 10000
threshold total-gprs-pdp-sessions

Configures thresholds for the total number of PDP contexts per GPRS sessions in the system.

**Product**
SGSN

**Privilege**
Administrator

**Syntax**

```
threshold total-gprs-pdp-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
The high threshold number of total PDP contexts per GPRS session for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 1 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of total PDP contexts per GPRS session for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 2000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition:** Actual total number of PDP Contexts ≥ High Threshold
- **Clear condition:** Actual total number of PDP contexts < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a total number of PDP contexts per GPRS session high threshold count of 10000 for a system using the Alert thresholding model:
threshold total-gprs-pdp-sessions 10000
threshold total-ha-sessions

Configures thresholds for the total number of HA sessions across all services in the system.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

threshold total-ha-sessions high_thresh [ clear low_thresh]

high_thresh
Default: 0
The high threshold number of HA sessions for all HA services that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
The low threshold number of HA sessions for all HA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the total number of HA sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HA sessions based on the following rules:
• Enter condition: Actual total number of HA sessions ≥ High Threshold
• Clear condition: Actual total number of HA sessions < Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a total number of HA sessions high threshold count of 10000 for an system using the Alert thresholding model:
threshold total-ha-sessions 10000
threshold total-hsgw-sessions

Configures thresholds for the total number of HSGW sessions across all services in the system.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
threshold total-hsgw-sessions high_thresh[ clear low_thresh]
```

**high_thresh**
Default: 0
The high threshold number of HSGW sessions for all HSGW services that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 1 through 1500000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
The low threshold number of HSGW sessions for all HSGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 1500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the total number of HSGW sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HSGW sessions based on the following rules:
- **Enter condition:** Actual total number of HSGW sessions ≥ High Threshold
- **Clear condition:** Actual total number of HSGW sessions < Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a total number of HSGW sessions high threshold count of 500000 for an system using the Alert thresholding model:
threshold total-hsgw-sessions 500000
threshold total-lma-sessions

Configures thresholds for the total number of LMA sessions across all services in the system.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```plaintext
threshold total-lma-sessions high_thresh [ clear low_thresh]
```

**high_thresh**

Default: 0
The high threshold number of LMA sessions for all LMA services that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 1 through 1500000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
The low threshold number of LMA sessions for all LMA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 1500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the total number of LMA sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for LMA sessions based on the following rules:

- **Enter condition:** Actual total number of LMA sessions ≥ High Threshold
- **Clear condition:** Actual total number of LMA sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a total number of LMA sessions high threshold count of 500000 for an system using the Alert thresholding model:
threshold total-lma-sessions 50000
threshold total-lns-sessions

Configures thresholds for the total number of LNS sessions in the system.

**Product**
PDSN, GGSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold total-lns-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  The high threshold number of total LNS sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Default: 0
  
  The low threshold number of total LNS sessions that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  The number can be configured to any integer value between 0 and 4000000. A value of 0 disables the threshold.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Monitor and set alarms or alerts when the total number of LNS sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of LNS sessions based on the following rules:

- **Enter condition**: Actual total number of LNS sessions ≥ High Threshold
  
- **Clear condition**: Actual total number of LNS sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll monitoring` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a total LNS session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-lns-sessions high_thresh 10000
```
threshold total-INS-sessions 10000
threshold total-mme-sessions

Use this command to configure thresholds for the total number of MME sessions across all the MME services in the system.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold total-mme-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0 (Disabled)

  The high threshold number of total MME sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

  The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.

- **clear low_thresh**

  Default: 0 (Disabled)

  The low threshold number of total MME sessions that maintains a previously generated alarm condition. If the number of MME sessions, across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.

  The number can be configured to any integer value between 0 and 4000000. A value of 0 disables the threshold.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to monitor and set alarms or alerts when the total number of MME sessions across all the MME services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of MME sessions based on the following rules:

- **Enter condition**: Actual total number of MME sessions ≥ High Threshold
- **Clear condition**: Actual total number of MME sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll total-mme-sessions` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

**Example**
The following command configures a total MME session high threshold count of 10000 for an system using the Alert thresholding model:

```
threshold total-mme-sessions 10000
```
threshold total-pdsn-sessions

Configures thresholds for the total number of PDSN sessions in the system.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold total-pdsn-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
The high threshold number of total PDSN sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
The low threshold number of total PDSN sessions that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the total number of PDSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of PDSN sessions based on the following rules:
- **Enter condition:** Actual total number of PDSN sessions \( \geq \) High Threshold
- **Clear condition:** Actual total number of PDSN sessions < Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a total PDSN session high threshold count of 10000 for an system using the Alert thresholding model:
threshold total-pdsn-sessions 10000
threshold total-pgw-sessions

Configures thresholds for the total number of P-GW sessions across all services in the system.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```c
threshold total-pgw-sessions high_thres[ clear low_thres]
```

<table>
<thead>
<tr>
<th>high_thres</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The high threshold number of P-GW sessions for all P-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.</td>
</tr>
<tr>
<td>The number can be configured to any integer value from 1 through 1500000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thres</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>The low threshold number of P-GW sessions for all P-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td>The number can be configured to any integer value between 0 and 1500000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

⚠️ **Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Monitor and set alarms or alerts when the total number of P-GW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for P-GW sessions based on the following rules:

- **Enter condition**: Actual total number of P-GW sessions ≥ High Threshold
- **Clear condition**: Actual total number of P-GW sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a total number of P-GW sessions high threshold count of 500000 for an system using the Alert thresholding model:
threshold total-pgw-sessions 50000
threshold total-sgw-sessions

Configures thresholds for the total number of S-GW sessions across all services in the system.

### Product

S-GW

### Privilege

Administrator

### Syntax

```
threshold total-sgw-sessions high_thresh[ clear low_thresh]
```

#### high_thresh

Default: 0
The high threshold number of S-GW sessions for all S-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.

The number can be configured to any integer value from 1 through 1500000. A value of 0 disables the threshold.

#### clear low_thresh

Default: 0
The low threshold number of S-GW sessions for all S-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

The number can be configured to any integer value between 0 and 1500000. A value of 0 disables the threshold.

---

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

### Usage

Monitor and set alarms or alerts when the total number of S-GW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for S-GW sessions based on the following rules:

- **Enter condition:** Actual total number of S-GW sessions ≥ High Threshold
- **Clear condition:** Actual total number of S-GW sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Example

The following command configures a total number of S-GW sessions high threshold count of 500000 for an system using the Alert thresholding model:
threshold total-sgw-sessions

threshold total-sgw-sessions 500000
threshold total-sgsn-sessions

Configures thresholds for the total number of SGSN sessions in the system.

Product
SGSN

Privilege
Administrator

Syntax

```
threshold total-sgsn-sessions high_thresh[ clear low_thresh]
```

### high_thresh

Default: 0
The high threshold number of total SGSN sessions for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.
The number can be configured to any integer value from 1 through 2000000. A value of 0 disables the threshold.

### clear low_thresh

Default: 0
The low threshold number of total SGSN sessions for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number can be configured to any integer value between 0 and 2000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

### Usage

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of SGSN sessions ≥ High Threshold
- **Clear condition:** Actual total number of SGSN sessions < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Example

The following command configures a total number of SGSN sessions high threshold count of 10000 for a system using the Alert thresholding model:
threshold total-sgsn-sessions 10000
threshold total-sgsn-pdp-sessions

Configures thresholds for the total number of PDP contexts per SGSN sessions in the system.

Product
SGSN

Privilege
Administrator

Syntax

```
threshold total-sgsn-pdp-sessions high_thresh[ clear low_thresh]
```

- **high_thresh**
  - Default: 0
  - The high threshold number of total PDP contexts per SGSN session for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.
  - The number can be configured to any integer value from 1 through 2000000. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - The low threshold number of total PDP contexts per SGSN session for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - The number can be configured to any integer value between 0 and 2000000. A value of 0 disables the threshold.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition**: Actual total number of PDP contexts ≥ High Threshold
- **Clear condition**: Actual total number of PDP contexts < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a total number of PDP contexts per SGSN session high threshold count of 10000 for a system using the Alert thresholding model:
threshold total-sgsn-pdp-sessions 10000
timestamps

Enables/disables the generation of a timestamp in response to each command entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects all future CLI sessions. Use the `timestamps` command in the Exec Mode to change the behavior for the current CLI session only.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
timestamps
no timestamps
```

Disables generation of timestamp output for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

**Usage**
Enable the timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

**Example**

```
timestamps
no timestamps
```
upgrade limit

Configures upgrade session limits, which are used to trigger the system as to when it may execute the software upgrade.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
upgradelimit [ timesession_life ] [ usagesession_num ]
```

- **upgradelimit**
  
  This command issued with no keywords sets all parameters to their defaults.

- **time session_life**
  
  Default: 120

  Defines the maximum number of minutes that a session may exist on the system, undergoing a software upgrade, before it is terminated by the system. As individual user sessions reach this lifetime limit, the system terminates the individual session(s). `session_life` must be an integer ranging from 1 through 1440.

- **usage session_num**
  
  Default: 100

  This keyword defines a low threshold limit of sessions running either on a PSC/PSC2 or system-wide. When a software upgrade is invoked, this parameter applies to the entire system. When the threshold is crossed (when the number of sessions on the PSC/PSC2 or system is less than this value), the remaining sessions on the card or system are terminated allowing the upgrade to begin. The remaining sessions on the PSC/PSC2 or system are terminated regardless of their session life. `session_num` must be an integer from 0 to 6000.

**Usage**

Use this command to configure upgrade session limits, which are used to trigger the system as to when it may execute the software upgrade.

**Important:** This command is not supported on all platforms.

**Important:** Software Patch Upgrades are not supported in this release.

**Example**

The following command sets the number of minutes a session can exist to `200` and the minimum number of sessions that may exist before terminating them to `50`:

```
upgrade limit time 200 usage 50
```
url-blacklisting database

This command configures URL Blacklisting database directory parameters.

Product
CF

Privilege
Security Administrator, Administrator

Syntax

```
url-blacklisting database { directory path path | max-versions max_versions | override file file_name }

default url-blacklisting database { directory path | max-versions | override file }
```

**default**
Configures the default values.

**directory path path**
Specifies the path to the directory to be used for storing URL Blacklisting databases.
path must be a string of 1 through 255 characters in length.
Default: /flash/bl

**max-versions max_versions**
Specifies the maximum number of URL Blacklisting database versions to be maintained in the URL Blacklisting database directory path with the base file name specified by the URL Blacklisting database override file.
max_versions must be an integer from 0 through 3.
Default: 0

**override file file_name**
Specifies the URL Blacklisting database override file name.
file_name must be in name.extension format. For example, abc.bin. And, must be a string of 1 through 10 characters in length.
Default: optblk.bin

Usage
Use this command to configure URL Blacklisting database directory parameters.

Example
The following command configures the maximum number of URL Blacklisting database versions to be maintained:

```
url-blacklisting database max-versions 3
```
Chapter 104
Global Title Translation Address-Map Configuration Mode Commands

The Global Title Translation (GTT) Address-Map configuration mode provides the commands to create, configure, and manage a specific GTT address map database.

- Exec Mode
  - configure
  - Global Configuration Mode
    - global title translation address-map instance instance
  - Global Title Translation Address-Map Configuration Mode

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

This command associates (links) the global title translation (GTT) address-map with a specific GTT association, which includes the translation action rules.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

\[
\text{associate \ gtt-association \ assoc\_num \ action \ id \ id}
\]

\[
\text{no \ association}
\]

\[
\text{no}
\]
Removes the association definition from the GTT address-map configuration.

\[
\text{gtt-association \ assoc\_num}
\]
Identifies a specific GTT association to link (associate) with the GTT address-map.
\*assoc\_num\* Must be an integer from 1 to 16.

\[
\text{action \ id \ id}
\]
Identifies a specific action defined in the GTT association database configuration.
\*id\* Must be an integer from 1 to 8.

Usage
Create an association between a specific translation action rule in a specific GTT association and this GTT address-map.

Example

\[
\text{associate \ gtt-association \ 1 \ action \ id \ 1}
\]
description

This command defines a descriptive string to facilitate identification of this particular global title translation (GTT) address-map. This is used for operator reference only.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

description string

no description

no
Removes the description string from the current global title translation address-map configuration.

string
Specifies the alphanumeric string that is stored. must be from 1 through 127 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

Usage
Use this command to set a description for reference by operators.

Example
description "GTT for Finnish national carrier."
end

Exits the configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
end
```

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the Global configuration mode.
gt-address

Configures the SCCP global title address.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

gt-address gt_address

no gt-address

no
Removes the GT address from the GTT address-map configuration.

gt_address
Up to 15 digits.

Usage
Define the SCCP short address.

Example

gt-address 01040552073424
mode

Configures the mode of operation of the SCCP entities.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

mode [ dominant | loadshare ]

  dominant
  This instructs the system to maintain the associated entity as the primary traffic pipe.

  loadshare
  This instructs the system to distribute the traffic load.

Usage
This command configure load balance for the system.

Example

mode loadshare
out-address

Identifies the out-going address of the SCCP entity. After this command is completed, the system enters the Out-Address configuration mode. Refer to the Out-Address Configuration Mode chapter for information about commands to define the out-address.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```plaintext
out-address name

no out-address
```

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the <code>out-address</code> definition from the GSS address-map configuration.</td>
</tr>
<tr>
<td>name</td>
<td>Defines a unique string to identify the out-going address using 1 to 63 alphanumeric characters.</td>
</tr>
</tbody>
</table>

Usage
Use this command to identify the address of the SCCP in the GTT configuration. This command also provides access to the Out-Address configuration mode so that the parameters for the out-going SCCP can be configured and maintained.

Example

```plaintext
out-address SCCP_London
```
Chapter 105
Global Title Translation Association Configuration Mode Commands

The Global Title Translation (GTT) Association configuration mode provides the commands to create the rules for translating the global titles (destination point codes and subsystem address in the messages) used for routing at the SCCP layer.

---

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

This command configures the actions that determine the operation of rules of the global title translation (GTT).

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
action id id type action_type start-digit value end-digit value
no action id id
```

- **id**
  id uniquely identifies an action. The id must be an integer from 1 to 8.

- **type action_type**
  The following defines the action rules that will determine how global titles (GT) are translated to locally understood addresses - in most cases point code (PC). The command can be re-issued multiple times to define multiple action rules.
  
  **constant**: Defines the starting digit in the range of digits in the incoming global titles that are translated to fixed addresses.
  
  **fixed**: Defines the starting digit in a fixed range of digits used for performing GTT.
  
  **gt-to-pc**: Use these digits as first of range of global title digits in incoming message to convert to point code for routing.
  
  **insert-pc**: Defines the rule for inserting destination point code before the incoming GTAI and change TT, ES and NAI. Use digits of incoming message global title digits as pc for routing.
  
  **selins**: Selective insertion type to perform GTT.
  
  **strip-pc**: Strip first 6 digits from GTAI if first 6 dgt in stripped point code are in INT format.
  
  **var-asc**: Use a variable number of digits, in ascending order, to perform GTT.
  
  **var-des**: Use a variable number of digits, in descending order, to perform GTT.

- **start-digit value**
  value must be an integer from 0 to 255.

- **end-digit value**
  value must be an integer from 0 to 255.

Usage

Create a global title translation rule that bases the translation on a fixed range of digits starting at 23 and ending at 122.

Example
action id 1 type fixed start-digit 23 end-digit 122
description

This command defines a descriptive string to facilitate identification of this particular global title translation (GTT) association. This is used for operator reference only.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

description string
no description

string
Specifies the alphanumeric string that is stored. must be from 1 through 127 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

no
Removes the description string from the current global title translation association configuration.

Usage
Use this command to set a description for reference by operators.

Example
The following command sets the description to identify a routing domain for messages transmitted within a national boundary.

description "GTT database 2"
end

Exits the configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the Global configuration mode.
gt-format

This command creates an instance of a global title formatting that is applied to the database in the process of address translation. Once the command is completed, the system enters global title (GT) format database configuration mode. The commands for configuration can be found in the GT Format Configuration Mode chapter in this reference guide.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gt-format format_num
```

- **format_num**
  1: Selects GT-format 1 options which include `nature-of-address` and `odd/even`. Once selected, the system enters GT-Format1 configuration mode.
  2: Selects GT-format2 options which include `translation-type`. Once selected, the system enters GT-Format2 configuration mode.
  3: Selects GT-format3 options which include `encoding-scheme`, `numbering-plan`, and `translation-type`. Once selected, the system enters GT-Format3 configuration mode.
  4: Selects GT-format4 options which include `encoding-scheme`, `nature-of-address`, `numbering-plan`, and `translation-type`. Once selected, the system enters GT-Format4 configuration mode.

Usage
Selects GT format #2 for the database GTT process.

Example

```
gt-format 2
```
variant

This command configures the choice of national standard protocols to associate with the GTT process databases.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
variant type
```

**default**
Sets the `variant` configuration to `itu`.

**type**
The following network variant national standards-based protocols are possible:

- `ansi`
- `china`
- `itu`
- `japan`

**Usage**
Use this command to select the national standard protocols to associate with the GTT process database.

**Example**
The following command sets the variant to `ansi`:

```
variant ansi
```
Chapter 106
GPRS Service Configuration Mode Commands

The GPRS Service Configuration Mode is used within the context configuration mode to define the criteria the SGSN needs to operate within a GPRS network. The GPRS Service works with other services, such as SGSN GPRS Tunneling Protocol (see SGTP Service Configuration Mode Commands) and Mobile Application Part (see MAP Service Configuration Mode Commands), to handle communication parameters required to work with other network entities such as the base station subsystem (BSS).

The prompt for this mode appears as:

```
[context_name]hostname(config-gprs-service)#
```

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

Defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
accounting { cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } + | context cntx_name }
default accounting cdr-types
no accounting { cdr-types | context }
```

**default**

Returns the system to default CDR generation which includes M-CDR, S-CDR, and SMS CDRs.

**no**

Disables all CDR types.

**cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr }**

Default: all types enabled.
Defines the types of CDRs to be generated within the specified GPRS service for accounting:

- **mcdr**: Enables generation of M-CDRs.
- **scdr**: Enables generation of S-CDRs.
- **sms**: Enables generation of SMS-type CDRs based on one of the following:
  - **mo-cdr**: SMS CDRs originates from the mobile.
  - **mt-cdr**: SMS CDRs terminates at the mobile.

**+**

This symbol indicates that more than one keyword can be used and repeated. This enables you to include more than one type of CDR selection in a single command.

**context cntx_name**

Specifies an accounting context to be associated with the GPRS service.

**cntx_name**: Define a string of 1 to 79 alphanumeric characters.

Usage
Use this command to define the type of CDRs to generate for GPRS service. By default all types of CDRs are generated. Note that change of this configuration will be applied to new calls and/or to new PDP contexts only.

By default, generation of the S-CDR, M-CDR, SMS-MT-CDR, and SMS MO-CDR types is enabled.

**Example**

The following command configures the system to generate only M-CDRs for accounting in the current GPRS service:

```
accounting cdr-types mcdr
```
associate-service

Identifies services to be associated with the GPRS Service.

**Important:** This command can be used before the associated service instance is created and configured but care should be used to match the service names.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] associate-service { gs name | map name | sgtp name } [ context ctxt_name ]
```

- **no**
  Removes the service association definition from the configuration.

- **gs name**
  Specifies which Gs service configuration, by naming the Gs service instance, to associate with this GPRS service.
  *name* must be a string of 1 to 63 alphanumeric characters with no spaces.

- **map name**
  Specifies which MAP service configuration, by naming the MAP service instance, to associate with this GPRS service.
  *name* must be a string of 1 to 63 alphanumeric characters with no spaces.

- **sgtp name**
  Specifies which SGTP service configuration, by naming the SGTP service instance, to associate with this GPRS service.
  *name* must be a string of 1 to 63 alphanumeric characters with no spaces.

- **context ctxt_name**
  Defines the context in which the service was created.
  *ctxt_name* must be a string of 1 to 63 alphanumeric characters with no spaces.

**Usage**

Use this command to associate other services, that have been or will be configured, to this GPRS service.
Example
The following command associates Gs service gs1 with this GPRS service.

    associate-service gs gs1 context sgsn2
cc profile

Configures the charging characteristic (CC) profile index properties.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
[ no ] cc profile index { buckets number | interval time | tariff time1 mins hours [ time2 mins hours [ time3 mins hours [ time4 mins hours ] ] ] | volume { downlink octets uplink octets | total octets } }

default cc profile index

no
Removes the a specific charging characteristics configuration definition.

default
Resets the charging characteristics to system defaults.

index
Configures a profile index for the parameter to be specified. index can be configured to any integer value from 0 to 15.

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

buckets number
Default: 4
Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.
number can be configured to any integer value from 1 through 4.

interval time
time is measured in seconds and can be configured to any integer value from 60 to 40,000,000.

tariff time1 mins hours time2 mins hours time3 mins hours time4 mins hours
Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.
GPRS Service Configuration Mode Commands

**Important:** The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:
- **mins:** The minutes of the hour, an integer value from 0 to 59.
- **hours:** The hour of the day, an integer value from 0 to 23.

```plaintext
volume { downlink vol_down_octets uplink vol_up_octets | total total_octets }
```

Specifies the downlink, uplink, and total volumes that must be met before closing a CDR.
- **vol_down_octets:** Measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.
- **vol_up_octets:** Measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.
- **total_octets:** The total traffic volume (up and downlink) measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.

**Usage**

Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the SGSN's charging characteristics. The SGSN supports up to 16 profile indexes. This command works in conjunction with the cc-sgsn command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts.

**Example**

The following command configures a profile index of 10 for tariff times of 7:00 AM and 7:30 PM:

```
cr profile 10 tariff time1 0 7 time2 30 19
```
check-imei-timeout-action

This command configures the action to be taken on the Gf interface if a Check-IMEI fails due to a timeout.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

check-imei-timeout-action [ continue | reject ]
default check-imei-timeout-action

default
Rejects the Attach or ISRAU procedure if a Check-IMEI timeout occurs.

continue
Instructs the SGSN to continue the Attach or ISRAU procedure if a Check-IMEI timeout occurs because the EIR is not reachable. This functionality matches standard call flow.

reject
Instructs the SGSN to reject the Attach or ISRAU procedure if a Check-IMEI timeout occurs.

Usage
Use this command to control the SGSN reaction if a Check-IMEI fails due to a timeout. The continue option allows the SGSN to go forward with the MS Attach if the first Check-IMEI fails to reach the EIR due to a timeout. Any subsequent activity (such as a RAU or Service Request) would force another Check-IMEI towards the EIR. If this subsequent MAP Check-IMEI should fail, then the same policy of continuing the procedure would apply.

Example
Use the following command to reject Attach Requests if the Check-IMEI timer runs out:

check-imei-timeout-action reject
ciphering-algorithm

This command configures the priority, ordering, for the use of the GPRS encryption ciphering algorithms.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

ciphering-algorithm priority priority algorithm

default ciphering-algorithm priority priority

default
Returns the system ciphering-algorithm priority to the default of GEA0 - which means that no ciphering will be done.

priority
Defines the priority or order of use for the ciphering algorithm. 
priority must be an integer from 1 to 8.

algorithm
Identifies the algorithm to be matched to the priority. Options include:

• gea0 - No ciphering
• gea1 - GPRS Encryption Algorithm - GEA1
• gea2 - GPRS Encryption Algorithm - GEA2
• gea3 - GPRS Encryption Algorithm - GEA3
• gea4 - GPRS Encryption Algorithm - GEA4 (not yet supported)
• gea5 - GPRS Encryption Algorithm - GEA5 (not yet supported)
• gea6 - GPRS Encryption Algorithm - GEA6 (not yet supported)
• gea7 - GPRS Encryption Algorithm - GEA7 (not yet supported)

Usage
Use this command to specify the order (priority) of usage for the GPRS encryption algorithms. All of the GPRS encapsulation algorithms use a 64-bit key derived from a common mechanism: the mobile receives a random challenge, then the SIM calculates an authentication signature and an encryption key.

Example
The following command sets no ciphering to be used after two encryption algorithms have been used:

ciphering-algorithm priority 3 gea0
dns israu-mcc-mnc-encoding

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

dns israu-mcc-mnc-encoding { decimal | hexadecimal }

default dns israu-mcc-mnc-encoding

default
Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

decimal
Default.
Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

hexadecimal
Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

Usage
Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query. For example:
In decimal, the MNC/MCC in a DNS query would appear like:

    rac0017.lac42e3.mnc310.mcc722.gprs

In hexadecimal, the MNC/MCC in a DNS query would appear like:

    rac0017.lac42e3.mnc0136.mcc02d2.gprs

Example
Use hexadecimal values for the MCC/MNC in the DNS query.

    dns israu-mcc-mnc-encoding hexadecimal
end

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

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Return to the Exec mode.
exit

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

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the context configuration mode.
gmm

This command defines the GPRS mobility management parameters for the SGSN service.

**Important:** The `gmm` command can be repeated to set each timer as needed.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gmm { accept-procedure [ new-tlli | old-tlli ] mobile-reachable-timeout mins | negotiate-t3314-timeout secs | purge-timeout mins | T3302-timeout mins | T3312-timeout mins | T3313-timeout secs | T3350-timeout secs | T3360-timeout secs | T3370-timeout secs | trau-timeout secs }
default gmm { mobile-reachable-timeout | negotiate-t3314-timeout | purge-timeout | T3302-timeout | T3312-timeout | T3313-timeout | T3350-timeout | T3360-timeout | T3370-timeout | trau-timeout }
no gmm negotiate-t3314-timeout

default
Resets the specified timer timeout to the system default.

no
Removes the specified GMM definition from the configuration.

accept-procedure [ new-tlli | old-tlli ]
Default: new-tlli
This keyword enables the use of either a new TLLI (temporary logical link identifier) or an old TLLI for attach-accept or RAU-accept messages sent by the SGSN to the MS during related procedures.

mobile-reachable-timeout mins
Default: 58 minutes
Timer value for the mobile reachability timer.
`mins` must be an integer from 4 to 1440.

negotiate-T3314-timeout secs
Set the number of seconds for the T3314-timeout ready timer value.
`secs` must be an integer from 0 to 11160. Default is 44 seconds.
- If the MS does not send the ready timer in the Attach/RAU request, then the SGSN sends this T3314-timeout (ready timer) value.
If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is less than or equal to the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the requested T3314 value.

If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is greater than the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the negotiate-T3314-timeout value.

**Important:** This is the only GMM timer that can be disabled by entering `no` at the beginning of the command syntax. `no gmm negotiate-t3314-timeout` By disabling negotiation of the T3314-timeout value, if the MS sends the requested value of the ready timer in the Att/RAU Request, then the SGSN sends the T3314-timeout value in the Att/RAU Accept.

---

**purge-timeout** *mins*

Default: 10080 minutes
Value defines the mm-context lifetime in minutes.
*mins* must be an integer from 1 to 20160.

**T3302-timeout** *mins*

Default: 12 minutes
Defines the number of minutes for timer to send to MS.
*mins* is an integer from 1 to 186.

**T3312-timeout** *min*

Default: 54 minutes
Periodic RAU update timer to send to MS.
*min* is an integer from 0 to 186.

**T3313-timeout** *secs*

Default: 5 seconds
Initial page timeout timer for retransmission for Paging Requests.
*secs* is an integer from 1 to 186.

**T3314-timeout** *secs*

Default: 44 seconds
Ready Timer for controlling Cell Update Procedure.
*secs* must be an integer from 0 to 500.

**T3350-timeout** *secs*

Default: 6 seconds
Retransmission timer for Attach Accept/RAU Accept/Ptmsi Realloc Command.
*secs* must be an integer from 0 to 20.

**T3360-timeout** *secs*

Default: 6 seconds
Retransmission timer for Authentication Request.
*secs* must be an integer from 0 to 20.
**T3370-timeout**  
Default: 6 seconds  
Retransmission timer for Identity Request.  
secs must be an integer from 0 to 20.

**trau-timeout**  
This timer is available in releases 9.0 and higher.  
Default: 30  
Specifies the number of seconds the “old” 3G SGSN waits to purge the MS’s data. This timer is started by the “old” SGSN after completion of the inter-SGSN RAU.  
secs: Must be an integer from 5 to 60.

**Usage**  
Use this command to set GMM timers.

**Example**  
Set the t3370 timer expiration for 15 seconds.  

```
gmm t3370-timeout 15
```
llc

Configures the timers that control the data flow for the logical link control (LLC) sub-layer.

---

**Important**: This command may be repeated as often as necessary to define the needed timers.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
llc { iov-ui-in-xid-reset | n201u-max } { sapi11 pkt-size | sapi3 pkt-size |
  sapi5 pkt-size | sapi9 pkt-size } | pdu-lifetime secs | t200 sapi1 time | t200 sapi11 time | t200 sapi13 time | t200 sapi15 time | t200 sapi7 time | t200 sapi9 time | uplink-pdu-len-validation }

default { iov-ui-in-xid-reset | n201u-max } { sapi11 | sapi3 | sapi5 | sapi9 |
  pdu-lifetime | T200 sapi1 | T200 sapi11 | T200 sapi13 | T200 sapi15 | T200 sapi7 | T200 sapi9 | uplink-pdu-len-validation }

no llc uplink-pdu-len-validation
```

---

**defaul**
Resets the configuration to the default values.

---

**no**
Disables the **uplink-pdu-len-validation**.

---

**iov-ui-in-xid-reset**
Available in 8.0 releases only.
This keyword makes it possible for the operator to configure whether or not to send IOV-UI in an XID-RESET. This is useful when the MS is not setup to accept IOV-UI (for example, MS sends Attach/RAU Requests with cksn=7) and including IOV-UI in the XID-Reset would result in Attach/RAU failure.
Default: Enabled

---

**n201u-max sapin pkt_size**
This keyword sets the maximum number of octets, per service access point identifier (SAPI), for the downlink data packets. This is the upper limit that the SGSN will negotiate with the subscriber for packets sent from the SGSN to the BSC.

- **sapin**: Command must identify one of the following SAPI: sapi11, sapi3, sapi5, or sapi9.
- **pkt_size**: Must be an integer from 140 to 1520. Default size is 1520 octets.
**pdu-lifetime secs**
Defines LLC layer PDU lifetime at the BSC.
*secs* must be an integer from 0 to 90.
Default: 6

**T200 sapi1 time**
Sets the retransmission timer (in seconds) for sapi1.
*time* must be an integer of 1 to 10.
Default: 5

**T200 sapi11 time**
Sets the retransmission timer (in seconds) for sapi11.
*time* must be an integer of 1 to 50.
Default: 40

**T200 sapi3 time**
Sets the retransmission timer (in seconds) for sapi3.
*time* must be an integer of 1 to 10.
Default: 5

**T200 sapi5 time**
Sets the retransmission timer (in seconds) for sapi5.
*time* must be an integer of 1 to 20.
Default: 10

**T200 sapi7 time**
Sets the retransmission timer (in seconds) for sapi7.
*time* must be an integer of 1 to 40.
Default: 20

**T200 sapi9 time**
Sets the retransmission timer (in seconds) for sapi9.
*time* must be an integer of 1 to 40.
Default: 20

**uplink-pdu-len-validation**
Available in releases 8.1 and higher.
This feature enables validation of the size of the uplink LLC packets. With validation enabled, the SGSN will drop any uplinked packets that are larger than the negotiated limit.
If the **no** form of the command is used, then this feature is disabled. The SGSN will be more flexible with uplink packet sizes. So if the SGSN and MS have a mismatch and the MS sends packets that are larger than expected, then the SGSN will not drop the packets.
Default: Enabled.

**Usage**
Use the command repeatedly to configure additional timers and features for the LLC sub-layer.
Example
Set the T200 retransmission timer to timeout at 12 seconds for SAPI5:

```plaintext
llc t200 sapi5 12
```

Use the following command to instruct the SGSN to ignore the N201_U packet size limits for uplink packets from an MS:

```plaintext
no uplink-pdu-len-validation
```
nri

This command configures the network resource identifier (NRI) to identify a specific SGSN. The NRI is stored in the P-TMSI. The SGSN uses a portion of this NRI to set the parameters for Gb flex (SGSN pooling) functionality.

Product

SGSM

Privilege

Security Administrator, Administrator

Syntax

nri length nri_length { nri-value nri_value | null-nri-value null_nri_value non-broadcast-lac lac_id rac rac_id { nri-value value } }

no nri

no

Removes the configured NRI value and location in P-TMSI for retrieval by this SGSN operator policy.

nri length nri_length

Specifies the number of bits to be used in the P-TMSI, bits 23 to 18, to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.

nri_length: Must be an integer from 1 to 6 to identify the number of bits.

null-nri-value null_nri_value

Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the sgsn offloading command, see the Exec Mode chapter).

null_nri_value: 0 (zero) indicates the keyword is not to be used and 1 to 63 are used to identify the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.

non-broadcast lac lac_id rac rac_id

Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure.

lac_id defines a location area code associated with a BSS. Must be an integer between 1 and 65535.

rac_id defines the remote area code to be associated with a BSS. Must be an integer between 1 and 255.

nri-value nri_value

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.

nri_value must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.

Multiple NRI values can be identified by providing multiple nri-values separated by a blank space for example: nri length 6 nri-value 29 43 61
Usage

Use this command to add or remove the Gb flex pool configuration for this GPRS service. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

Example

The following command specifies the the NRI length as 5 bits, identifies SGSN 23 with LAC 222 and RAC 12 for offloading procedure with NRIs 6 and 41:

```
nri length 5 null-nri-value 34 non-broadcast lac 222 rac 12 nri-value 6 41
```
paging-policy

Configures the paging parameters for the GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

paging-policy { last-known-area { all | bsc | cell | location-area | routing-area } + | max-retransmissions:retran_num}

no paging-policy last-known-area { bsc | cell | location-area | routing-area }

default paging-policy { last-known-area | max-retransmissions } 

no
Disables the paging-policy definition for this GPRS service configuration.

default
Resets the defaults for parameters managed by this paging policy.

last-known-area
Select one or more paging areas and enter them in preferred paging order:
• all : Pages in the last known BSC.
• bsc : Pages in last known BSC.
• cell : Pages in last known cell.
• location-area : Pages in last known location area.
• routing-area : Pages in last known routing area.

By default, paging occurs in the following order:
cell, BSC, routing area, location area.

max-retransmission retn_num

Configures the maximum number of retries for a page request per paging area.

retn_num: Enter an integer from 0 to 5.
• 2 : default.
• 0 : disables retransmission for paging request so that the SGSN only sends a single 2G PS-paging request to the BSC with no retransmissions.

+ Keywords can be repeated or combined as needed to complete the paging policy configuration.
Usage
Use this command to configure the order of preference for retransmitting into specified paging-areas.

Example
Use the following command to instruct the SGSN to page the cell and BSC as the last-known areas:

```
paging-policy last-known-area cell bsc
```
**peer-nsei**

This command associates a peer (remote) network service entity (NSEI) for a BSS with this GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
peer-nsei nse_id { lac lac_id rac rac_id | pooled }

[ no ] peer-nsei nse_id { lac lac_id rac rac_id | pooled }
```

- **no**
  Removes the NSEI LAC/RAC or pooling configuration from this BSS peer configuration.

- **nse_id**
  Defines the NSEI for this GPRS service.
  *nse_id* must be an integer from 0 to 65535.

- **lac lac_id**
  Defines a location area code associated with the NSE BSS.
  *lac_id* must be an integer between 1 and 65535.

- **rac rac_id**
  Defines the remote area code to be associated with the NSE BSS.
  *rac_id* must be an integer between 1 and 255.

- **pooled**
  Enables pooling with non-pooled BSCs within the pool area.

**Usage**

Use this command repeatedly to associate one or more LAC/RAC combinations and/or pooling with this peer-GPRS service configuration.

The Network Service Entity (NSE) at the BSS and the SGSN provides the network management functionality required for the operation of the Gb interface. Each NSE is identified by means of NSE identifier (NSEI).

**Example**

The following command configures the NSE with identifier as 4114 having location area code 234 and routing area code as 22:

```
peer-nsei 4114 lac 234 rac 22
```

The following command enables Gb flex (pooling) functionality for this GPRS service:
peer-nsei 4114 pooled
plmn

This command identifies the Public Land Mobile Network (PLMN) for the GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
plmn id mcc mcc_num mnc mnc_num

no plmn id
```

```
no
Removes the PLMN information from the configuration for the current SGSN service.
```

```
mcc mcc_num
Define the mobile country code (MCC) portion of the PLMN Id.
mnc_num must be a 3 digit integer from 100 to 999.
```

```
mnc mnc_num
Define the mobile network code (MNC) portion of the PLMN Id.
mnc_num must be a 2 or 3 digit integer from 00 to 999.
```

Usage
Use this command to set PLMN parameters for the current SGSN service.

Example
The following command identifies the PLMN MCC as 200 and the MNC as 10:

```
plmn id mcc 200 mnc 10
```
**setup-timeout**

This command configures the maximum number of seconds allowed for session setup.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
setup-timeout seconds
```

```
default setup-timeout
```

**default**

Returns the configuration to the default, 60 seconds.

**seconds**

An integer from 1 to 100000.

**Usage**

Use this command to set the time allowed for session setup.

**Example**

The following command sets the maximum session setup time to 300 seconds:

```
setup-timeout 300
```
sgsn-context-request

This command specifies whether or not the PTMSI signature check should be skipped if the PTMSI signature is not included in the SGSN context request.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sgsn-context-request ptmsi-signature-absence allowed
no sgsn-context-request ptmsi-signature-absence allowed
default sgsn-context-request ptmsi-signature-absence
```

- **no**
  - Removes this definition from the system configuration.

- **default**
  - Returns the configuration to the default action to perform the PTMSI signature check.

**Usage**
Use this command to skip the PTMSI signature check.

**Example**
The following command instructs the system to perform the PTMSI signature check.

```
default sgsn-context-request ptmsi-signature-absence
```
sgsn-number

Define the SGSN E.164 number to be used when interacting via MAP protocol for this GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sgsn-number sgsn_number
no sgsn-number
```

**Usage**

Use this command to identify the ISDN number for the SGSN associated with this GPRS service.

**Example**

Disable the E.164 number for this GPRS service.

```
no sgsn-number
```
**sm**

This command configures the session management (SM) parameters associated with this particular GPRS service context.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sm { activate-max-retransmissions num_retries | deactivate-max-retransmissions num_retries |
ignore-pco-decode-error | modify-max-retransmissions num_retries |
partial-apn-match | requested-apn-from-first-subrec | t3385-timeout secs |
t3386-timeout secs | t3395-timeout secs | trim-trailing-spaces-in-apn }
```

```
default sm { activate-max-retransmissions | deactivate-max-retransmissions | 
ignore-pco-decode-error | modify-max-retransmissions | t3385-timeout | t3386-
timeout | t3395-timeout | trim-trailing-spaces-in-apn }
```

**default**

Resets the SM parameters to the defaults.

**activate-max-retransmissions num_retries**

Defines the maximum number of retries to transmit ‘activate PDP context request’.

- `num_retries`: Must be an integer from 1 to 10.
- Default: 4

**deactivate-max-retransmissions num_retries**

Defines the maximum number of retries to transmit ‘deactivate PDP context request’.

- `num_retries`: Must be an integer from 1 to 10.
- Default: 4

**ignore-pco-decode-error**

Enables the SGSN to ignore received decode errors that are due to incorrectly encoded PCO IE length in SM Requests.

- Default: disabled

**modify-max-retransmissions num_retries**

Defines the maximum number of retries to transmit ‘modify PDP context request’.

- `num_retries`: integer from 1 to 10.
- Default: 4

**partial-apn-match**

Enables partial matching of requested APN during APN selection.
Partial APN or APN with trailing spaces may be present in an Activate Request because incorrect information was keyed in by the user. Though it is valid to reject such Activation Requests, it increases the signaling between the MS and the SGSN. This has an impact on the radio resources.

**requested-apn-from-first-subrec**

Enables use of a ‘requested APN’ from the first subscription record. When this feature is enabled, the PDP Activation is not rejected during APN Selection; instead, the APN from the first subscription record is used as the requested APN and the SGSN continues with the rest of the APN Selection process.

A requested APN is an optional IE in an Activate PDP Request. To get the requested PDP type, if multiple PDP subscription records exist for the subscriber, then the MS has to include the APN information to choose the PDP subscription record during APN selection. Otherwise, such activations will be rejected during APN selection (per TS 23.060 Appendix A). Though it is valid to reject such activation requests, it increases the signaling between the MS and the SGSN, which impacts the radio resources.

**t3385-timeout secs**

Defines the maximum amount of time for retransmission of ‘activate request’ messages.

*secs*: Must be an integer from 1 to 60.

Default: 8

**t3386-timeout secs**

Defines the maximum amount of time for retransmission of ‘modify request’ messages.

*secs*: Must be an integer from 1 to 60.

Default is 8 seconds.

**t3395-timeout secs**

Defines the maximum amount of time for retransmission of ‘deactivate request’ messages.

*secs*: Must be an integer from 1 to 60.

Default: 8

**trim-trailing-spaces-in-apn**

Enables SGSN to strip off any trailing space(s) in requested APN.

If a requested APN in an Activate PDP Context Request has any trailing spaces, then those trailing spaces will be removed and the length field will be updated.

**Usage**

Repeat this command with different keywords (parameters) to configure the SM (session management) as needed for this GPRS service. Keywords can be used to optimize signaling between the MS and the SGSN to reduce the impact on the radio resources.

**Example**

Reset the number of retransmission messages for deactivate PDP context request to 5.

```
sm deactivate-max-retransmissions 5
```
**sndcp**

Define the SNDCP reassembly-timeout interval associated with this GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
sndcp reassembly-timeout time

default sndcp reassembly-timeout
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Resets the timer configuration to the default value.</td>
</tr>
<tr>
<td><code>time</code></td>
<td>Defines the interval. <code>time</code>: Must be an integer from 1 to 5. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to modify the SNDCP reassembly timer.

**Example**
Reset the default for the timer.

```plaintext
default sndcp reassembly-timeout
```
Chapter 107
GRE Tunnel Interface Configuration Mode Commands

The Generic Routing Encapsulation (GRE) Tunnel Interface Configuration Mode is used to create and manage the GRE tunneling interfaces for addresses, address resolution options, etc.

![Diagram]

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

This command configures the destination IPv4 address of the tunnel by specifying the IPv4 destination end address. This is a mandatory configuration for GRE tunnel interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] destination address ip_address
```

- **no**
  Removes/disassociates the configured destination IP address from specific GRE tunnel interface configuration.

- **address ip_address**
  Configures the IP address for the interface specifying the IPv4 IP address.
  *ip_address* must be specified using the standard IPv4 dotted decimal notation.

**Usage**

Use this command to configure the destination IPv4 address of the tunnel by specifying the IP address of destination tunnel end for GRE tunnel interface.

**Important**: State of source address will affect the operational state of the tunnel.

**Example**

The following command sets the 1.2.3.4 as destination IP address of the GRE tunnel interface:

```
destination address 1.2.3.4
```
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the Interface Configuration Mode and returns to the Context Configuration Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the context configuration mode.
keepalive

This command configures various parameters for sending Keepalives to the remote end-point in GRE tunnel interface configuration. By default sending keepalives is disabled.

Product
All

Privilege
Security Administrator, Administrator

Syntax

keepalive [interval time_interval num-retry retry]

[default | no] keepalive

default
Sets the sending of Keepalives with default parameters.
interval: 10 seconds
num-retry: 3 retries

no
Disables the keepalive and turns off the sending of Keepalives messages.

interval time_interval
Default: 10
Specifies the time interval (in seconds) between two Keepalives sent to remote ends of GRE tunnel interface configuration.
time_interval must be an integer from 5 through 3600.

num-retry retry
Default: 3
Specifies number of retransmission of keepalives to remote node without getting any response before the remote node is marked as dead/down.
retry must be an integer between 0 through 10.

Usage
Use this command to configure the parameters for sending Keepalives to the remote end-point of GRE tunnel. It also configures the interval at which GRE Keepalives are sent on the interface and number of retries without getting a response from the remote end-point before the tunnel is shutdown. By default, Keepalives will not be sent.

Example
The following command enables the keepalive and sets the other parameters to defaults:

default keepalive
keepalive
source

This command configures the source IPv4 address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IPv4 interface. This is a mandatory configuration for GRE tunnel interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[no] source {address ip_address | interface interface_name}

- **no**
  Removes/disassociates the configured source IP address or host interface from specific GRE tunnel interface configuration.

- **address ip_address**
  Configures the IP address for the interface specifying the IPv4 IP address.
  *ip_address* must be specified using the standard IPv4 dotted decimal notation.

- **interface interface_name**
  Specifies the name of the preconfigured non-tunnel IPv4 interface, whose address is used as the source address of the GRE tunnel.

Usage
Use this command to configure the source IPv4 address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IPv4 interface for GRE tunnel interface.

**Important:** State of source address will affect the operational state of the tunnel.

Example
The following command sets the 1.2.3.4 as source IP address of the GRE tunnel interface:

```
source address 1.2.3.4
```
tos

This command configures the parameters/action for the TOS parameter in the IPv4 tunnel transport protocol header.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip tos {value [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value] | copy}
```

no ip tos

**default**
Sets the IP TOS to lower bits value of 0.

**value [tos_value]**
Default: af11
Specifies the IP QoS DSCP per-hop behavior to be marked on the outer header of signalling packets originating from the Access Gateway. This is a standards-based feature (RFC 2597). The following forwarding types are supported:

- **af11**: Designates the use of Assured Forwarding 11 per-hop behavior
- **af12**: Designates the use of Assured Forwarding 12 per-hop behavior
- **af13**: Designates the use of Assured Forwarding 13 per-hop behavior
- **af21**: Designates the use of Assured Forwarding 21 per-hop behavior
- **af22**: Designates the use of Assured Forwarding 22 per-hop behavior
- **af23**: Designates the use of Assured Forwarding 23 per-hop behavior
- **af31**: Designates the use of Assured Forwarding 31 per-hop behavior
- **af32**: Designates the use of Assured Forwarding 32 per-hop behavior
- **af33**: Designates the use of Assured Forwarding 33 per-hop behavior
- **af41**: Designates the use of Assured Forwarding 41 per-hop behavior
- **af42**: Designates the use of Assured Forwarding 42 per-hop behavior
- **af43**: Designates the use of Assured Forwarding 43 per-hop behavior
- **be**: Designates the use of Best Effort forwarding per-hop behavior
- **ef**: Designates the use of Expedited Forwarding per-hop behavior typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

<table>
<thead>
<tr>
<th></th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Drop</strong></td>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
<td>AF41</td>
</tr>
<tr>
<td><strong>Medium Drop</strong></td>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
<td>AF42</td>
</tr>
<tr>
<td><strong>High Drop</strong></td>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
<td>AF43</td>
</tr>
</tbody>
</table>

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.
**lower-bits** *tos_value*

Default: 0
Sets the least-significant 6 bits in the TOS byte with the specified numeric value.
*tos_value* must be an integer from 0 through 255.

**copy**

This keyword instructs the system to copy the TOS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the TOS value of the IPv4 tunnel transport protocol header.

**Usage**

Use this command either to set the TOS parameter in the IPv4 tunnel transport protocol header to the specified value or instructs to copy the TOS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the TOS value of the IPv4 tunnel transport protocol header. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the TOS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the TOS byte.

**Example**

The following command instructs the system to copy the TOS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the TOS value of the IPv4 tunnel transport protocol header:

```
tos copy
```
ttl

This command configures the Time to live (TTL) parameter to be used in the tunnel transport protocol header for the current GRE tunnel interface.

### Product
All

### Privilege
Security Administrator, Administrator

### Syntax
```
ttl ttl_value
```
```
default ttl
```

```
default
Sets the TTL value to system default value; i.e. 15.
```

```
ttl_value
Default: 15
Specifies the maximum time to live to be used in the tunnel transport protocol header
The time to live (TTL) is not a measure of time but the number of hops through the network.
ttl_value must be an integer between 1 through 255.
```

### Usage
Use this command to set the TTL parameter to be used in tunnel transport protocol header for GRE tunnel configuration.

### Example
The following configures the IP address to associate with the interface:
```
ttl 10
```
The Group of Ruledefs Configuration Mode is used to configure groups of ruledefs. This mode is accessed by entering the group-of-ruledefs command in the Active Charging Service Configuration Mode.

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

This command enables adding/removing ruledefs in the current group-of-ruledefs.

**Important:** A maximum of 128 ruledefs can be added to a group-of-ruledefs.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Syntax**

```
add-ruledef priority priority ruledef ruledef_name
no add-ruledef priority priority
```

- **no**
  Specifies that the ruledef associated with the specified priority number is to be removed from the current group-of-ruledefs.

- **priority priority**
  Specifies priority of a ruledef in the current group-of-ruledefs. `priority` must be unique in the group-of-ruledefs, and must be an integer from 1 through 10000.

- **ruledef ruledef_name**
  Specifies name of the ruledef to add to the current group-of-ruledefs. `ruledef_name` must be the name of a ruledef, and must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

Use this command to add/remove ruledefs from a group-of-ruledefs. A group-of-ruledefs may contain optimizable ruledefs. Whether a group is optimized or not is decided on whether all the ruledefs in the group-of-ruledefs can be optimized, and if the group is included in a rulebase that has optimization turned on, then the group will be optimized. When a new ruledef is added, it is checked if it is included in any group-of-ruledefs, and whether it needs to be optimized, etc.

**Example**

The following command adds the ruledef `ruledef23` to the current group-of-ruledefs, and assigns it a priority of 3:

```
add-ruledef priority 3 ruledef ruledef23
```
end

This command returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to change to the Exec mode.
exit

This command exits the Group of Ruledefs Configuration mode and returns to the Active Charging Service Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the Active Charging Service Configuration mode.
**group-of-ruledefs-application**

This command specifies the purpose of setting up a group-of-ruledefs as either for charging or for post processing.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
  group-of-ruledefs-application { charging | post-processing }

  no group-of-ruledefs-application
```

- **no**
  - Removes the group-of-ruledefs-application configuration from the current group-of-ruledefs.

- **charging**
  - Specifies that the current group-of-ruledefs is for charging purpose.

- **post-processing**
  - Specifies that the current group-of-ruledefs is for post-processing purpose.

**Usage**

Use this command to specify the purpose of setting up a group-of-ruledefs as either for charging or for post processing. If not configured, by default the rule-application type will be charging.

**Example**

The following command configures the current group-of-ruledefs as for post-processing purpose:

```
group-of-ruledefs-application post-processing
```
Chapter 109
Gs Service Configuration Mode Commands

The Gs Service configuration mode configures the parameters used to setup and maintain a Gs interface for a connection between the SGSN and an MSC/VLR.

```
Exec Mode
| configure
  | Global Configuration Mode
  | context name
  | Context Configuration Mode
  | gs-service name
  | Gs Service Configuration Mode

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
```
### associate-sccp-network

This command associates a previously defined Signaling Connection Control Part (SCCP) network instance with the Gs service. This association is required to access Visitor Location Register(s) (VLRs).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
associate-sccp-network sccp_net_id
no associate-sccp-network
```

- **no**
  Removes the associated SCCP network configuration instance from this Gs service configuration.

- **sccp_net_id**
  Identifies the SCCP network configuration instance to associate with this Gs interface to enable connection with VLR(s).

  - `sccp_network_num`: Must be an integer from 1 through 12.

**Usage**

Use this command to associate the SCCP network configuration instance with the Gs interface in this service.

**Important:** A single SCCP network configuration instance can not be shared with multiple Gs services.

**Important:** To enable a Gs service, the user needs to configure `ssn` with the `bssap+` command.

**Example**

Following command associates SCCP network 2 with this Gs service.

```plaintext
associate-sccp-network 2
```
bssap+

This command defines the Base Station System Application Part Plus configuration parameters for the Gs service to enable the SGSN to access a Visitor Location Register(s) (VLRs).

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] bssap+ ssn ss_num

no
Removes the configured BSSAP+ subsystem number from this Gs service.

ssn ss_num
Specifies the subsystem number to configure in this Gs interface to use BSSAP+.
ss_num must be an integer from 1 through 255.

Usage
Use this command to configure the BSSAP+ subsystem with Gs interface in this service to communicate with VLR(s).

Important: A single SCCP network configuration instance can not be shared with multiple Gs services.

Important: To start a Gs service, the user needs to configure the command parameter.

Example
Following command configures subsystem 101 with BSSAP+ in this Gs service.

bssap+ ssn 101
**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```  

**Usage**

Return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the previous configuration mode.
max-retransmission

This command configures the retransmission values for different procedure counters in Gs service as described in TS 29.018.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

max-retransmissions { n8 | n9 | n10 | n12 } retrans_num

default max-retransmissions { n8 | n9 | n10 | n12 }

no
Removes the configured Gs procedures from this Gs service.

{ n8 | n9 | n10 | n12 }
Specifies the various Gs service procedures that are available to be used to communicate with VLR(s).

- n8: Defines the maximum number of retries for explicit IMSI detach from a non-GPRS service. Default is 2.
- n9: Defines the maximum number of retries for implicit IMSI detach from the GPRS service. Default is 2.
- n10: Defines the maximum number of retries for BSSAP+ to send Reset Indication messages. Default is 2.
- n12: Defines the maximum number of retries for BSSAP+ to send Reset Indication messages. Default is 2.

retrans_num
Default: 2
Specifies the number of re-transmission of message for specified procedures.
retrans_num Must be an integer from 0 through 10.

Usage
Use this command to configure the retransmission values for specific procedure counters in Gs service. counters are based on TS 29.018. This command can be entered for each procedure counter separately.

Example
Following command configure retransmission value as 3 for counter for procedure to send BSSAP+ Reset Indication messages in this Gs service.

max-retransmissions n12 3
non-pool-area

This command creates a non-pool area for a set of subscriber location area code (LAC) values that can be used with a specific VLR for the Gs service.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Syntax**

non-pool-area non_pool_name { use-vlr vlr_name lac lac_num }+
no non-pool-area non_pool_name

---

**no**
Removes the configured non-pool area from this Gs service.

---

**non_pool_name**
Specifies the name of the non-pool area to configure with this command.  
non_pool_name must be an alpha and/or numeric string of 1 to 63 characters.

---

**use-vlr vlr_name**
Specifies the name of the VLR to be associated with this non-pool area.  
vlr_name is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.

---

**lac lac_num**
Specifies the subscribers’ location area code to be attached with this non-pool area and specific VLR. This LAC of subscriber is obtained from the radio area indicator (RAI).  
lac_num is the LAC value and must be an integer value from 1 through 65535.

---

More than one of the above keywords can be entered within a single command.

**Usage**

Use this command to specify the non-pool area containing VLR name to use for a set of LAC. This command can be used multiple times, subject to a limit of 32 LAC values (the total for non-pool-area and pool-area configurations) per Gs service.

**Example**

Following command configure a non-pool area starpool1 to use VLR named starvrl1 for LAC 101 in a Gs service.

non-pool-area starpool1 use-vlr starvrl1 lac 101
**pool-area**

This command creates a pool area configuration instance. This command also enters the Pool Area configuration mode to define the set of VLRs to use for a pool area for a set of subscriber location area code (LAC) values in the Gs service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
pool-area pool_name [-noconfirm ]
```

```
no pool-area non_pool_name
```

- **no**
  Removes the configured pool area from this Gs service.

- **pool_name**
  Specifies the name of the pool area to configure with this command for VLR pooling and association of a LAC.
  
  `pool_name`: Must be an alpha and/or numeric string of 1 to 63 characters.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create/enter the pool area configuration mode. This mode is used configure the set of VLRs to be used for a set of subscriber LAC. This command can be used multiple times, subject to a limit of 32 LAC values (the total number of `non-pool-area` and `pool-area` configurations) per Gs service.

**Example**

The following command configures a pool area named `starpool1` in a Gs service without any confirmation prompt.

```
pool-area starpool1 -noconfirm
```
sgsn-number

Define the SGSN’s E164 number to associate an SGSN with this Gs Service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sgsn-number E.164_number
```

<table>
<thead>
<tr>
<th>E.164_number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the SGSN’s ‘telephone’ number, the ISDN number for per ITU-T E.164 numbering plan. The number must be a numerical string of 1 to 15 digits.</td>
</tr>
</tbody>
</table>

Usage
For releases 8.1 or higher, use this command to define the SGSN’s E.164 ISDN number. This value should match the `sgsn-number` defined for SGSN Service or GPRS Service.

**Important:** Note: the Gs Service will not start unless the SGSN’s E.164 number is configured.

Example

```
sgsn-number 12345678901234
```
timeout

This command configures various timers defining the wait before retransmitting a specific message for Gs service procedures.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
timeout { t6-1-timer t6_1_dur | t8-timer t8_dur | t9-timer t9_dur | t10-timer t10_dur | t12-1-timer minute t12_1_dur | t12-2-timer t12_2_dur }

[ default ] timeout { t6-1-timer | t8-timer | t9-timer | t10-timer | t12-1-timer | t12-2-timer }
```

default

Sets the timer value to wait in seconds/minutes to default values. Default values for timers are:

- **t6-1-timer**: 10 seconds
- **t8-timer**: 4 seconds
- **t9-timer**: 4 seconds
- **t10-timer**: 4
- **t12-1-timer**: 54 mins (+ 8 seconds)
- **t12-2-timer**: 4 seconds

---

t6-1-timer t6_1_dur

Default: 10
Specifies the retransmission timer value to guard the location update.

`t6_1_dur` is the waiting duration in seconds before retransmitting the specific message and must be an integer from 10 through 90.

---

t8-timer t8_dur

Default: 4
Specifies the retransmission timer value to guard the explicit IMSI detach from the GPRS service procedure.

`t8_dur` is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

---

t9-timer t9_dur

Default: 4
Specifies the retransmission timer value to guard the explicit IMSI detach from the non-GPRS service procedure.

`t9_dur` is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.
**t10-timer** t10_dur
Default: 4
Specifies the retransmission timer value to guard the implicit IMSI detach from the GPRS service procedure. t10_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

**t12-1-timer** minute t12_1_dur
Default: 54 minutes (plus 8 seconds for transmission delay)
Specifies the retransmission timer value to control the resetting of SGSN-Reset variable procedure. t12_1_dur is the waiting duration in minutes before retransmitting reset message for the SGSN Reset variable and must be an integer from 0 through 380.

**t12-2-timer** t12_2_dur
Default: 4
Specifies the retransmission timer value to guard the SGSN reset procedure. t12_2_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

**Usage**
Use this command to configure the time, for different procedure timers, to wait before retransmitting a procedure message.
This command can be repeated for each timer to configure multiple timers.

**Example**
Following command sets the timeout duration of 4 seconds for t8 timer to wait before retransmitting the procedure message to explicitly do the IMSI detach from GPRS service:

```
default timeout t8-timer
```
vlr

This command defines a VLR configuration for use with this Gs service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
vlr vlr_name isdn-number E164_num [ bssap+ ssn ssn ] [ point-code pt_code ]

no vlr vlr_name
```

**vlr_name**
Specifies the name of the VLR to configure in this Gs mode with ISDN number.

**isdn-number**
Specifies the VLR number to configure with this command.

**bssap+ ssn ssn**
Specifies the subsystem number to configure with this VLR to use BSSAP+.

**point-code**
Specifies SS7 address of VLR in point code value to this configured VLR name.

**Usage**
Use this command to define VLR configuration instances to be associated with the Gs service.

A maximum of 32 VLRs can be configured per Gs service.

**Example**
Following command configures the VLR named starvlr1 with an ISDN number 12344567, a subsystem number of 252, and a point code value of 123.345.567:

```
vlr starvlr1 isdn-number 12344567 point-code 123.345.567
```
Chapter 110
GT-Format1 Configuration Mode Commands

The GT-Format1 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

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

Exits the configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the Global configuration mode.
nature-of-address

Configures the indicator to identify the nature of the address.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
nature-of-address ( international | national | subscriber )
```

- **international**
  
  Identifies the numbers as international.

- **national**
  
  Identifies the numbers as matching the national configuration.

- **subscriber**
  
  Identifies the numbers as subscriber numbers.

**Usage**

Configure the identify of the GT format as national.

**Example**

```
nature-of-address national
```
**odd-even-indicator**

Configures the bits for matching the global title translation.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
odd-even-indicator type
```

- **type**
- **odd**: Sets the odd bit for matching the GTT.
- **even**: Sets the even bit for matching the GTT.
Chapter 111
GT-Format2 Configuration Mode Commands

The GT-Format2 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

```
Exec Mode
  configure
    Global Configuration Mode
      gtt association id
        GTT Association Configuration Mode
          gt-format 2
            GT-Format2 Configuration Mode
```

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

Exits the configuration mode and returns to the Exec mode.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the Global configuration mode.
translation-type

Configures the translation type to be applied during the translation process.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

\texttt{translation-type \textit{number}}

\textit{number}
Must be an integer between 0 and 255.
Default is 0

Usage
Use this command to configure the GTT translation type to be applied during global title translation process.

Example

\texttt{translation-type 232}
Chapter 112
GT-Format3 Configuration Mode Commands

The GT-Format3 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

```
Exec Mode

configure

Global Configuration Mode

gtt association id

GTT Association Configuration Mode

gt-format 3

GT-Format3 Configuration Mode
```

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

Configures the encoding-scheme to use during global title translation (GTT).

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
encoding scheme scheme_type
```

- `scheme_type`

Select one of the following encoding scheme types to determine the encoding type to be used during GTT:
- `bcd-even`: BCD even encoding scheme
- `bcd-odd`: BCD odd encoding scheme
- `nw-specific`: Network specific encoding scheme
- `unknown`: Unknown encoding scheme

Usage
Select BCD even encoding for GTT

Example

```
encoding scheme bcd-even
```
end

Exits the configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
end
```

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the Global configuration mode.
numbering-plan

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

numbering-plan plan_type

plan_type
Select one of the following numbering plans be employed during GTT:
• data: Data numbering plan
• generic: Generic number plan
• isdn: ISDN tel numbering plan
• isdn-mobile: ISDN mobile numbering plan
• land-mobile: Land mobile numbering plan
• maritime-mobile: Maritime mobile numbering plan
• nw-specific: Private network / network-specific numbering plan
• telex: Telex numbering plan
• unknown: Unknown numbering plan

Usage
Select ISN telephone number plan for GTT process.

Example
The following command sets the numbering plan to use during GTT processing to isdn

numbering-plan isdn
**translation-type**

Configures the global title translation (GTT) process to apply a specific number for translation during the GTT process.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
translation-type number
```

*number*

Must be an integer between 0 and 255. Default is 0

**Usage**

Use this command to define the translation-type to be used during the global title translation process.

**Example**

```
translation-type 233
```
Chapter 113
GT-Format4 Configuration Mode Commands

The GT-Format4 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

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

Configures the encoding-scheme to use during GTT.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
encoding scheme scheme_type
```

- **scheme_type**
  Select one of the following encoding scheme types to determine the encoding type to be used during GTT:
  - `bcd-even`: BCD even encoding scheme
  - `bcd-odd`: BCD odd encoding scheme
  - `nw-specific`: Network-specific encoding scheme
  - `unknown`: Unknown encoding scheme

**Usage**
Select BCD even encoding for GTT

**Example**

```
encoding scheme bcd-even
```
end

Exits the configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the Global configuration mode.
nature-of-address

Configures the indicator to identify the nature of the address.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
nature-of-address ( international | national | subscriber )
```

- **international**
  Identifies the numbers as international.

- **national**
  Identifies the numbers as matching the national configuration.

- **subscriber**
  Identifies the numbers as subscriber numbers.

Usage

Configure the identify of the GT format as national.

Example

```
nature-or-address national
```
numbering-plan

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

numbering-plan plan_type

- **plan_type**
  Select one of the following numbering plans be employed during GTT:
  - **data**: Data numbering plan
  - **generic**: Generic number plan
  - **isdn**: ISDN tel numbering plan
  - **isdn-mobile**: ISDN mobile numbering plan
  - **land-mobile**: Land mobile numbering plan
  - **maritime-mobile**: Maritime mobile numbering plan
  - **nw-specific**: Private network/ network-specific numbering plan
  - **telex**: Telex numbering plan
  - **unknown**: Unknown numbering plan

Usage

Select ISN telephone number plan for GTT process.

Example

numbering-plan isdn
translation-type

Configures the GTT process to apply a specific number for translation during the GTT process.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
translation-type number
```

- `number`
  Must be an integer between 0 and 255.
  Default is 0.

Usage
Use this command to configure the translation-type to be implemented during the global title translation process.

Example

```
translation-type 231
```
Chapter 114
GTPP Server Group Configuration Mode Commands

The GTPP Server Group Configuration Mode is used to create and manage the GTPP server groups within the context or system.

GTPP server group commands facilitate the setup of the SMC hard disk for CDR storage. As well, for accounting and charging functionality within a context, these commands can be used to configure the management of a group (list) of charging gateway function (CGF) servers on a per subscriber or per GGSN APN level.

In this mode, your prompt will be similar to `/context_name>hostname(config-gtpp-group)#`
gtpp attribute

Enables the specification of some of the optional fields in the CDRs that the GSN (GGSN or SGSN) generates and/or how the information is to be presented.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | misisdn | node-id-suffix STRING | plmn-id | rat | record-extensions | sms { destination-number | recording-entity | service-centre } } +
```

```
no gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | misisdn | node-id-suffix | plmn-id | rat | record-extensions | rat | sms { destination-number | recording-entity | service-centre } }
```

```
default gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | misisdn | plmn-id | rat | record-extensions | sms { destination-number | recording-entity | service-centre } }
```

---

default

 Resets the default attribute values for this GTPP group configuration.

---

no

 Disables the specified optional field so that the information will not be present in generated CDRs.

---

cell-plmn-id

SGSN only
Default: Disabled
Enter this keyword to enable the system to include the Cell PLMN ID field in the M-CDR.

---

diagnostics

Default: Disabled
Enter this keyword to enable the system to include the Diagnostic field in the CDR that is created when PDP contexts are released. The field will include one of the following values:

- **26** - For GGSN: if the GGSN sends “delete PDP context request” for any other reason (e.g., the operator types “clear subscribers” on the GGSN). For SGSN: The SGSN includes this cause code in the S-CDR to indicate that a secondary PDP context activation request or a PDP context modification request has been rejected due to insufficient resources.

- **36** - For GGSN: this cause code is sent in the G-CDR to indicate the PDP context has been deactivated in the GGSN due to the SGSN having sent a “delete PDP context request” to the GGSN. For SGSN, this cause code is used to indicate a regular MS or network-initiated PDP context deactivation.
- 37 - when the network initiates a QoS modification, the SGSN sends in the S-CDR to indicate that the MS initiation deactivate request message has been rejected with QoS not accepted as the cause.

- 38 - if the GGSN sends “delete PDP context request” due to GTP-C/GTP-U echo timeout with SGSN. If the SGSN sends this cause code, it indicates PDP context has been deactivated due to path failure, specifically GTP-C/GTP-U echo timeout.

- 39 - SGSN only - this code indicates the network (GGSN) has requested a PDP context reactivation after a GGSN restart.

- 40 - if the GGSN sends “delete PDP context request” due to receiving a RADIUS Disconnect-Request message.

duration-ms
Default: Disabled
Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require).

imei
Default: Disabled
For SGSN: includes the IMEI value in the S-CDR.
For GGSN: includes the IMEISV value in the G-CDR.

local-record-sequence-number
Default: Disabled
This keyword provides both the local record sequence number and the Node ID. In the x-CDRs, this field indicates the number of CDRs generated by the node and is unique within the session manager. The Node ID field is included in the x-CDR for any of several reasons, such as when PDP contexts are released or if partial-CDR is generated based on configuration. The field will consist of a AAA Manager identifier automatically appended to the name of the SGSN or GGSN service. The name of the SGSN or GGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.

**Important:** If this keyword is enabled and the `gtpp centralized-lrsn-creation` option is enabled with the `gtpp single-source centralized-lrsn` command, then the Node ID format changes as follows.

- `<1-byte-AAProxy-restart-counter> <3-byte AAProxy instance number> <node-id-suffix>` If “centralized-lrsn-creation” is not enabled, then node-id format for CDRs generated by Sessmgr is as follows.

  - `<1-byte Sessmgr restart-value> <3-byte Sessmgr instance number> <node-id-suffix>` If “centralized-lrsn-creation” is not enabled, then node-id format for CDRs generated by ACSMgr is as follows.

  - `<1-byte ACSmgr restart-value> <3-byte ACSmgr instance number>` <Active charging service-name>

msisdn
Default: Enabled
For SGSN: includes the MSISDN value in the S-CDR.
For GGSN: includes the MSISDN value in the G-CDR.

node-id-suffix STRING
Default: Disabled
Specifies the string suffix to use in the NodeID field of GTPP CDRs. Each Session Manager task generates a unique NodeID string per GTPP context.

**STRING:** This is the configured Node-ID-Suffix having any string between 1 to 16 characters.

**Important:** The NodeID field is a printable string of the nddddSTRING format: n: The first digit is the Sessmgr restart counter having a value between 0 and 7. ddd: The number of sessmgr instances. Uses the specified NodeID-suffix in all CDRs. The “Node-ID” field consists of sessMgr Recovery counter (1 digit) n + AAA Manager identifier (3 digits) ddd + the configured Node-id-suffix (1 to 16 characters) STRING. If the centralized LRSN feature is enabled, the “Node-ID” field will consist of only the specified NodeID-suffix (NodeID-prefix is not included). If this option is not configured, then GTPP group name will be used instead (For default GTPP groups, context-name will be used).

**Important:** If this node-id-suffix is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group named as the node-id-suffix.

<table>
<thead>
<tr>
<th>plmn-id [ unknown-use ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: Enabled</td>
</tr>
<tr>
<td>For SGSN, reports the SGSN PLMN Identifier value (the RAI) in the S-CDR provided if the dictionary supports it.</td>
</tr>
<tr>
<td>For GGSN, reports the SGSN PLMN Identifier value (the RAI) in the G-CDR if it was originally provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one. Normally when SGSN PLMN-id information is not available, the attribute sgsnPLMNIdentifier is not included in the CDR. This keyword enables the inclusion of the sgsnPLMNIdentifier with a specific value when the SGSN PLMN-id is not available.</td>
</tr>
<tr>
<td>unknown-use hex_num must be a hexadecimal number from 0x0 through 0xFFFFFFFF to identify a foreign SGSN that has not provided a PLMN-id. For GGSN only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>rat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: Enabled</td>
</tr>
<tr>
<td>For SGSN: includes the RAT (identifies the radio access technology type) value in the S-CDR.</td>
</tr>
<tr>
<td>For GGSN: includes the RAT (identifies the radio access technology type) value in the G-CDR.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>record-extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: Disabled</td>
</tr>
<tr>
<td>Enables network operators and/or manufacturers to add their own recommended extensions to the CDRs according to the standard record definitions from 3GPP TS 32.298 Release 7 or higher.</td>
</tr>
</tbody>
</table>

| sms { destination-number | recording-entity | service-centre } |
|----------------------|
| This keyword is specific to the SGSN. |
| Entering this keyword causes the inclusion of an SMS-related field in the SMS-MO-CDR or SMS-MT-CDR. |
| destination-number - Entering this option includes the "destinationNumber" field in the SMS-MO-CDR or SMS-MT-CDR. |
| recording-entity - Entering this option includes the "recordingEntity" field in the SMS-MO-CDR or SMS-MT-CDR. |
| service-centre - Entering this option includes the "serviceCentre" field in the SMS-MO-CDR or SMS-MT-CDR. |

| + |
| Indicates that this command can be entered multiple times to configure multiple attributes. |
Usage
This command dictates some of the optional information fields that should be reported in CDRs generated by the GGSN. In addition, it controls how the information for some of the mandatory fields are reported. Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).

Example
The following command dictates that the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtp attribute duration-ms
```
gtpp charging-agent

Configures the IP address and port of the system interface within the current context used to communicate with the CGF or the GSS.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp charging-agent address ip_address [ port port ]
nogtpp charging-agent

no
Removes a previously configured charging agent address.

address ip_address
Specifies the IP address of the interface configured within the current context that is used to transmit G-CDR records to the CGF or the GSS.

ip_address must be configured using dotted decimal notation.

port port
It is an optional parameter. It specifies the Charging Agent UDP port. If port is not defined, the IP will take the default port number 49999.

Default: 49999

port must be followed by an integer, ranging from 1 to 65535.

Important: Configuring GTPP charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address.

Usage
This command can be used to establish a UDP interface to connect to the GSS or this command can establish a Ga interface to connect to the CFG. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the gtpp commands in this chapter).

This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GGSN/SGSN is known to the CGF or the GSS. Therefore, the IP address used for the Ga or UDP interface could be identical to one bound to a GGSN/SGSN service (a Gn interface).

If no GGSN/SGSN services are configured in the same context as the Ga/UDP interface, the address configured by this command is used to receive unsolicited GTPP packets.

Example
The following command configures the system to use the interface with an IP address of 192.168.13.10 as the accounting interface with port 20000 to the CGF:

```
gtp charging-agent address 192.168.13.10

gtp charging-agent address 192.168.13.10 port 20000
```
gtpp data-request sequence-numbers

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp data-request sequence-numbers start { 0 | 1 }
default gtpp data-request sequence-numbers start
```

**default**
Default is 0 (zero).

**start { 0 | 1 }**
Specifies the value of the start sequence number for the GTPP Data Record Transfer Request. Default: 0

- `0` = Designates the start sequence number as 0.
- `1` = Designates the start sequence number as 1.

Usage

When the GGSN/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that can not properly handle the re-use of sequence number 0 in the echo request packets.

Example

The following command sets the sequence to start at 1.

```
gtpp data-request sequence-numbers start 1
```
**gtpp deadtime**

Configures the amount of time the GGSN/SGSN waits before attempting to communicate with a CGF that was previously marked as unreachable (non-responsive).

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp deadtime time

default deadtime
```

| default
| Resets the deadtime to the default of 120 seconds.

| time
| Default: 120
| Specifies the amount of time that must elapse before the system attempts to communicate with a CGF that was previously unreachable.
| time is measured in seconds and can be configured to any integer value from 1 to 65535.

**Usage**
If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down.
This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.
Refer to the `gtpp detect-dead-server` and `gtpp max-retries` commands for additional information on the process the system uses to mark a CGF as down.

**Example**
The following command configures the system to wait 60 seconds before attempting to re-communicate with a CGF that was marked as down:

```
gtpp deadtime 60
```
gtpp dead-server suppress-cdrs

This command configures the action the GGSN or the SGSN will take on CDRs generated during a communication failure between the GGSN or the SGSN and the GTPP servers.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | default ] gtpp dead-server suppress-cdrs
```

- **no**
  Removes the suppression instruction from the configuration and sets the CDR suppression mode as disabled.

- **default**
  Resets the GGSN or the SGSN to the default mode: disable suppression of CDRs when GTPP server detected as “dead” or unreachable.

**Usage**

*For the GGSN:* This command works in conjunction with the `gtpp detect-dead-server` to set an action when a communication failure is detected between the GGSN and a configured GTPP server. It disables the archiving of CDRs on the system when the GTPP server is unreachable or dead.

*For the GGSN and the SGSN:* Typically, during a communication or server failure, the GGSN or SGSN retains the GTPP requests until the system buffer runs out of resources. This command enables suppression of the CDRs, so with this command the GGSN or the SGSN will start purging all CDRs associated with this GTPP group as soon as the GGSN/SGSN detects that the GTPP server is down or that a communication failure has occurred. The CDRs generated, for the period while the server is down/unreachable, will also be purged.

**Example**
The following command configures the system to start purging CDRs when a communication failure with a server is detected:

```
gtpp dead-server suppress-cdrs
```
**gtpp detect-dead-server**

Configures the number of consecutive communication failures that could occur before the system marks a CGF as ‘dead’ (unreachable).

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp detect-dead-server consecutive-failures max_number

default gtpp detect-dead-server consecutive-failures
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the system to the default number of consecutive failures.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>consecutive-failures  max_number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 5</td>
</tr>
<tr>
<td>Specifies the number of failures that could occur before marking a CGF as down. If 0 (zero) is the value entered, then the system will mark the CGF as dead after a single instance of max-retries has been attempted with no success, regardless of configured deadtime. max_number could be configured to any integer value from 0 to 1000.</td>
</tr>
</tbody>
</table>

**Usage**
This command works in conjunction with the gtpp max-retries parameter to set a limit to the number of communication failures that can occur with a configured CGF. The gtpp max-retries parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The gtpp detect-dead-server parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicate with the CGF of next highest priority. If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority CGF again. If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active. Refer to the gtpp max-retries command for additional information.

**Example**
The following command configures the system to allow 8 consecutive communication failures with a CGF before it marks it as down:

```
gtpp detect-dead-server consecutive-failures 8
```
gtpp dictionary

This command designates specific dictionary used by GTPP for specific context.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp dictionary {custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom4 | custom5 | custom6 | custom7 | custom8 | custom9 | standard}

default gtpp dictionary
```

```
default
Configures the default dictionary.
```

```
custom1
Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.
```

```
custom2
Custom-defined dictionary.
```

```
custom3
Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 but it does support the encoding of IP addresses in binary format for CDRs.
```

```
custom4
Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 except that:
  ● the Data Record Format Version information element contains 0x1307 instead of 0x1308
  ● “QoSRequested” is not present in the LoTV containers
  ● “QoSnegotiated” is added only for the first container and the container after a QoS change
```

```
custom5 ... custom20
Custom-defined dictionaries.
```

```
custom21 ... custom25
Custom-defined dictionaries for GGSN only.
```
**gtpp dictionary**

---

**custom26**
Custom-defined dictionary for customization of G-CDR records for GGSN only. This is compliant to 3GPP TS 32298 (R6 v 6.5.0) for proprietary fields and encoding.

---

**custom27**
Custom-defined dictionary for customization of S-CDR records for SGSN only. This is compliant to 3GPP TS 32298 (R6 v 6.6.0) for proprietary fields and encoding.

---

**custom28 ... custom30**
Custom-defined dictionaries for GGSN only.

---

**standard**
Default: Enabled
A dictionary conforming to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

---

**Usage**
Use this command to designate specific dictionary used by GTPP for specific context.

---

**Example**
The following command configures the system to use custom3 dictionary to encode IP address in Binary format in G-CDRs:

```
gtpp dictionary custom3
```
**gtpp duplicate-hold-time**

This command configures the number of minutes to hold onto CDRs that are possibly duplicates while waiting for the primary CGF to come back up.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gtpp duplicate-hold-time minutes minutes
default gtpp duplicate-hold-time
```

**default**
Resets the configuration to the default value of 60 minutes for the duplicate hold time.

**minutes**
When the primary CGF is down, the number of minutes to hold onto CDRs that may be duplicates.

*minutes* must be an integer from 1 to 10080. Default is 60.

**Usage**
Use this command to configure how long to hold onto CDRs, that are possibly duplicates, while waiting for the primary CGF to come back up. If the GGSN determines that the primary CGF is down, CDRs that were sent to the primary CGF, but not acknowledged, are sent by the GGSN to the secondary CGF as “possibly duplicates”. When the primary CGF comes back up, the GGSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

**Example**
Use the following command to set the amount of time to hold onto CDRs to 2 hours (120 minutes):

```plaintext
gtpp duplicate-hold-time minutes 120
```
gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp echo-interval time
{default | no} gtpp echo-interval

default
Resets the configuration to the default echo-interval of 60 seconds.

no
Disables the use of the echo protocol except for the scenarios described in the Usage section for this command.

time
Specifies the number of seconds for sending GTPP echo packets.
time must be an integer from 60 to 3600. Default: 60

Usage
The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:
- Upon system boot
- Upon the configuration of a new CGF server on the system using the gtpp server command as described in this chapter
- Upon the execution of the gtpp test accounting command as described in the Exec Mode Commands chapter of this reference
- Upon the execution of the gtpp sequence-numbers private-extensions command as described in this chapter

The echo-interval command is used in conjunction with the gtpp max-retries and gtpp timeout commands as described in this chapter.
In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.
The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the gtpp deadtime command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.
Example
The following command configures an echo interval of 120 seconds:

```
gtp echo-interval 120
```
gtpp egcdr

Configures the eG-CDR parameters and triggers.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```

default gtpp egcdr {final-record include-content-ids only-with-traffic closing-cause same-in-all-partials | losdv-max-containers | lotdv-max-containers | service-idle-timeout 0}

no gtpp egcdr service-data-flow threshold {interval | volume { downlink [uplink ] | total | uplink [downlink]}}
```

- **final-record [ closing-cause [ same-in-all-partials | unique ] | include-content-ids [ all | only-with-traffic ] ]**

  Enables configuration of the final eG-CDR.

  - **closing-cause** - Configures closing cause for the final eG-CDR.
  - **same-in-all-partials** - Specifies that the same closing cause is to be included for multiple final eG-CDRs.
  - **unique** - Specifies that the closing cause for final eG-CDRs is to be unique.
  - **include-content-ids** - Controls which content-ids are being included in the final eG-CDR.
  - **all** - Specifies that all content-ids be included in the final eG-CDR.
  - **only-with-traffic** - Specifies that only content-ids with traffic be included in the final eG-CDRs.

- **losdv-max-containers number**

  The maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR. number can be configured to any integer value from 1 to 255.

  Default: 10

- **lotdv-max-containers number**

  The maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR. number can be configured to any integer value from 1 to 8.

  Default: 8
service-data-flow threshold [ interval seconds | volume { downlink | total | uplink } bytes ]

Configures the thresholds for closing a service data flow container within an eG-CDR.
- interval - configures the time interval in seconds
- volume - can specify uplink or downlink or combined total (uplink + downlink) byte thresholds.

A service data flow container has statistics for an individual content-id. When the threshold is reached, the service data flow container is closed.
Default: disabled

service-idle-timeout seconds

Specifies a time period where if no data is reported for a service flow, then the service container is closed and added to eG-CDR (as part of LOSDV container list) with service condition change as ServiceIdleOut.
seconds can be configured to any integer value from 10 to 86,400.
Default: 0. This means there is no service-idle-timeout trigger.

Usage
Use this command to configure individual triggers for eG-CDR generation.

Example
Use the following command to set the maximum number of LoSDV containers to 7.

    gtpp egcdr losdv-max-containers 7
**gtpp error-response**

This command configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp error-response { discard-cdr | retry-request }

default gtpp error-response
```

- **default**
  Resets the system’s configuration to the default value for error-response. Default is retry-request.

- **discard-cdr**
  Instructs the system to purge the request upon receipt of an error response and not to retry.

- **retry-request**
  Instructs the system to retry sending a DRT after receiving an error response. This is the default behavior.

**Usage**

This command configures the system’s response to receiving an error message after sending a DRT request.

**Example**

```
gtpp error-response discard-cdr
```
gtpp max-cdrs

Configures the maximum number of charging data records (CDRs) to be included in a packet.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtp max-cdrs number_cdrs [ wait-time seconds ]
default gtpp max-cdrs

default
Sets the default configuration.

number_cdrs
Default: 1
Specifies the maximum number of CDRs to insert in a single packet must be an integer from 1 to 255.

wait-time seconds
Default: Disabled
Configures the number of seconds the GSN waits to send the packet while accumulating CDRs as defined by max-cdr. If the wait-time interval expires before max-cdrs is reached, then this keyword over-rides and the packet is sent.
seconds any integer from 1 to 300.

Important: wait-time interval can only be enabled if the value for max-cdrs number_cdrs is greater than 1.

Usage
The system places CDRs into a packet until either max-cdrs is met, wait-time times out, or the maximum PDU size, configured by the gtpp max-pdu-size command, is met.
The gtpp max-pdu-size and the wait-time parameters take priority over max-cdrs.

Important: This command’s configuration is ignored if CDRs are stored on an SMC hard disk.

Example
The following command configures the system to place a maximum of 10 CDRs in a single GTPP packet with a wait-time of 30 seconds:

    gtpp max-cdrs 10 wait-time 30
**gtpp max-pdu-size**

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
gtpp max-pdu-size pdu_size
default gtpp max-pdu-size
```

- **default**
  Resets the default `max-pdu-size` of 4096.

- **pdu_size**
  Default: 4096
  Specifies the maximum payload size of the GTPP packet. The payload includes the CDR and the GTPP header.
  `pdu_size` is measured in octets and can be configured to any integer value from 1024 to 65400.

**Usage**

The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and sends the packet containing the one CDR regardless.

The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR.

The system performs standard IP fragmentation for packets that exceed the system’s maximum transmission unit (MTU).

**Important:** The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system’s `max-pdu-size` doesn't include the IPv4 and UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).

**Example**
The following command configures a maximum PDU size of 2048 octets:

```bash
gtpp max-pdu-size 2048
```
**gtp max-retries**

Configures the maximum number of times the system attempts to communicate with an unresponsive CGF.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtp max-retries max_attempts
```

**default gtp max-retries**

---

```
default
```

Resets the system's **max-retries** to the default of 4.

```
max_attempts
```

Default: 4

Specifies the number of times the system attempts to communicate with a CGF that is not responding. **max_attempts** can be configured to any integer value from 1 to 15.

**Usage**

This command works in conjunction with the **gtpp detect-dead-server** and **gtpp timeout** parameters to set a limit to the number of communication failures that can occur with a configured CGF. When the value specified by this parameter is met, a failure is logged. The **gtpp detect-dead-server** parameter specifies the number of consecutive failures that could occur before the server is marked as down. In addition, the **gtpp timeout** command controls the amount of time between re-tries. If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system’s memory buffer is exceeded. Refer to the **gtpp detect-dead-server** and **gtpp timeout** commands for additional information.

**Example**
The following command configures the maximum number of re-tries to be 8.

```
gtp max-retries 8
```
gtpp mbms bucket

This command configures the traffic data volume (bucket) limit of charging buckets due to QoS changes of tariff time that can occur before a G-MBMS-CDR should be closed.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp mbms buckets number
[ no ] gtpp mbms buckets

no
Disables the configured traffic data volume bucket limits trigger for G-MBMS-CDR generation for MBMs user service data.

buckets number
Default: 4
Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before a G-MBMS-CDR should be closed.

number can be configured to any integer value from 1 through 4.

Usage

Use this command to configure the traffic data volume (bucket) based G-MBMS-CDR generation triggers for MBMS user data service.

Example

The following command configures the bucket-based trigger to generate G-MBMS-CDRs after changes in 2 container:

   gtpp mbms buckets 2
gtpp mbms interval

This command configures the interval duration for interval-based triggers for GTPP MBMS Charging Data Record (G- MBMS-CDR) generation.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp mbms interval duration_sec
no gtpp mbms interval
```

- **no**
  Disables the interval-based trigger for G- MBMS-CDR generation for MBMs user service data.

- **interval duration_sec**
  Default: Disabled
  Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions occur:
  - Downlink traffic volume is reached within the time interval
  - Tariff time based trigger occurred within the time interval
  - Data volume (up and downlink) bucket trigger occurred within the time interval
  
  *duration_sec* is measured in seconds and can be configured to any integer value from 60 through 40,000,000.

Usage

Use this command to configure the G- MBMS-CDR generation triggers for MBMS user data service.

Example

The following command configures the interval-based trigger to generate G- MBMS-CDRs in every 60 seconds:

```
gtpp mbms interval 60
```
**gtpp mbms tariff**

This command configures the tariff slots for tariff-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gtpp mbms tariff time1 mins hours [ time2 mins hours [ time3mins hours [ time4mins hours ] ] ]
[ no ] gtpp mbms tariff
```

- **no**
  - Disables the tariff-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

- **t tariff time1 mins hours [ time2 mins hours [ time3mins hours [ time4mins hours ] ] ]**
  - Default: Disabled
  - Specified time-of-day time values to close the current statistics container (but not necessarily the accounting record).

**Important:** The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:
- **mins**: The minutes of the hour, an integer value from 0 through 59.
- **hours**: The hour of the day, an integer value from 0 through 23.

**Usage**
Use this command to configure the tariff-time-based triggers for G-MBMS-CDR generation in MBMS user data service.

**Example**
The following command configures the tariff-time-based trigger to generate G-MBMS-CDRs every day at 11 hours and 30 min:

```plaintext
gtpp mbms tariff time1 30 11
```
gtpp mbms volume

This command configures the download traffic data volume based trigger for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp mbms volume download_bytes
[ no ] gtpp mbms volume
```

**no**
Disables the configured download traffic data volume based trigger for G-MBMS-CDR generation for MBMS user service data.

**volume download_bytes**
Default: Disabled
Specifies the threshold of downlink data volumes that must be met before a G-MBMS-CDR should be closed. `download_bytes` is the total download traffic volume measured in octets and can be configured to any integer value from 100,000 through 4,000,000,000.

Usage
Use this command to configure the traffic data volume (download) based G-MBMS-CDR generation triggers for MBMS user data service.

Example
The following command configures the traffic data volume (download) limit to trigger to generate G-MBMS-CDRs after reaching 150,000 octets:

```
gtpp mbms volume download_bytes
```
gtpp redirection-allowed

Configures the system to allow/disallow the redirection of CDRs when the primary CGF is unavailable.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

[ default | no ] gtpp redirection-allowed

default
Resets the system to allow redirection of CDRs.

no
Removes the redirection definition from the configuration.

Usage
This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the **no gtpp server** command. This functionality is enabled by default.

If the **no gtpp redirection-allowed** command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, the system will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.

Example
The following command configures the system to allow the redirection of CDRs when the primary CGF is unavailable:

```
default gtpp redirection-allowed
```
gtpp redirection-disallowed

This command has been obsoleted and is replaced by the gtpp redirection-allowed command.
gtpp server

Configures the charging gateway function (CGF) accounting server(s) with in GTPP server group that the system is to communicate with.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp server ip_address [ max msgs ] [ priority priority ] [ udp-port port ] [ node-alive { enable | disable } ] [-noconfirm ]

no gtpp server ip_address [ udp-port port ]

no
Deletes a previously configured CGF.

ip_address
Specifies the IP address of the CGF in dotted decimal notation for IPv4 or colon notation for IPv6.

max msgs
Default: 256
Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets.
msgs can be configured to any integer value from 1 to 256.

priority priority
Default: 1000
Specifies the relative priority of this CGF. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to.
priority can be configured to any integer value from 1 to 1000. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the -noconfirm option, you are not asked for confirmation and multiple servers could be assigned the same priority.

udp-port port
Default: 3386
Specifies the UDP port over which the GGSN communicates with the CGF. port can be configured to any integer value between 1 and 65535.

node-alive { enable | disable }
Default: Disable.
This optional keyword allows operator to enable/disable GGSN to send Node Alive Request to GTPP Server (i.e. CGF). This configuration can be done per GTPP Server basis.
-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Use this command to configure the CGF(s) that the system sends CDR accounting data to. Multiple CGFs can be configured using multiple instances of this command subject to the following limits:
- Up to 4 CGFs can be configured in one GTPP server group
- Total 32 CGFs can be configured per context.

Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of "1" has the highest priority.

Important: The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

Example
The following command configures a CGF with an IP address of 192.168.2.2 and a priority of 5.

```
gtpp server 192.168.2.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of 100.10.35.7:

```
no gtpp server 100.10.35.7
```
gtpp source-port-validation

This command configures whether the system validates the UDP source port in received GTPP messages.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no | default] gtpp source-port-validation
```

- **no**
  Validates the IP source address but not the UDP source port.

- **default**
  Restores this parameter to its default setting of enabled.

**Usage**
This command configures whether the system validates the UDP source port in received GTPP messages.

**Example**
The following command disables UDP port validation:

```
no gtpp source-port-validation
```
gtpp storage-server

Configures information for the GTPP back-up storage server.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp storage-server  ip_address  port  port_num
no gtp storage-server  ip_address  port  port_num
```

**no**
Removes a previously configured back-up storage server.

**ip_address**
The IP address of the back-up storage server expressed in dotted decimal notation.

**port  port_num**
Default: 3386
Specifies the UDP port number over which the GGSN communicates with the back-up storage server.

Usage
This command identifies the connection to the GSS. One backup storage server can be configured per GTPP group.

Example
The following command configures a GSS with an IP address of 192.168.1.2:

```
gtpp storage-server  192.168.1.2
```
gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

gtpp storage-server local file { compression { gzip | none } | format { custom1 | custom2 | custom3 | custom4 | custom5 | custom6 | custom7 | custom8 } | name prefix prefix | purge-processed-files | rotation { cdr-count count | time-interval time [force-file-rotation] | volume size } }

default gtpp storage-server local file { compression | format | name prefix | purge-processed-files | rotation { cdr-count | time-interval | volume } }

no gtpp storage-server local file rotation { purge-processed-files | rotation { cdr-count | time-interval } }

no
Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.

compression { gzip | none }

Configures the type of compression to be used on the files stored locally.
gzip – Enables Gzip file compression.
none – Disables Gzip file compression - this is the default value.

format custom1 .. 8

Configures the file format to be used to format files to be stored locally.
custom1 – File format custom1 - this is the default file format.
custom2 to custom5 Customer specific CDR file formats.
custom6 – File format custom6 with a block size of 8K for CDR files.
custom7 – File format custom7 is a customer specific CDR file format.
custom8 – File format custom8 is a customer specific CDR file format. It uses node-id-suffix_date_time_fixed-length-seq-num format for file naming where:

- date is date in MMDDYYYY (01312010) for mat
- time is time in HHMMSS (023508) format
- fixed-length-seq-num is the fixed length of sequence number for specific file having 6 digit counter starting from 000001 and end to 999999. Once file sequence reached to 999999 the sequence will be reset to 000001.

name prefix prefix

Defines the prefix to be used for the file name. By default the file name prefix would be ‘GTPP-group-name + VPN-ID’.
prefix— Enter a string of 1 to 64 alphanumeric characters.

    purge-processed-files [ purge-interval purge_dur ]

Default: Disabled
Enables the GSN to periodically delete locally processed (*.p) CDR files from the HDD on the SMC card.

**Important:** This option is available only when GTPP server storage mode is configured for local storage of CDRs with the `gtpp storage-server mode local` command.

`purge-interval purge_dur` provides an option for user to control the purge interval duration in minutes by setting `purge_dur`.
`purge_dur` must be an integer from 1 through 259200.
Default: 60 minutes

**rotation**

    rotation { cdr-count count | time-interval time [ force-rotation ] | volume size }

Specifies rotation related configuration for GTPP files stored locally.
`cdr-count count` - Configure the CDR count for the file rotation. Enter a value from 1000 to 65000. Default value 10000.
`time-interval time` - Configure the time interval for file rotation. Enter a value in seconds ranging from 30 to 86400. Default value is 3600 seconds (1 hour).
`force-file-rotation` - Force CDR file-rotation at specified interval, configured with `time-interval time` keyword, even if there are no CDRs generated. By default this keyword is “Disabled”.
`volume size` - Configure the file volume, in MB, for file rotation. Enter a value ranging from 2 to 40. This trigger can not be disabled. Default value is 10MB.

**Usage**

This command configures the parameters for storage of GTPP packets as files on the local server - meaning the hard disk.

**Example**

The following command configures rotation for every 1.5 hours for locally stored files.

    gtpp storage-server local file rotation time-interval 5400
gtpp storage-server max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp storage-server max-retries max_attempts

default gtpp storage-server max-retries
```

- **default**
  Restores the system to the default value of 2 retry attempts.

- **max_attempts**
  Default: 2
  Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding.
  `max_attempts` can be configured to any integer value from 1 to 15.

**Usage**

This command works in conjunction with the `gtpp storage-server timeout` parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server. The `gtpp storage-server` timeout command controls the amount of time between re-tries. Refer to the `gtpp storage-server` timeout command for additional information.

**Example**
The following command configures the maximum number of re-tries to be 8.

```
gtpp storage-server max-retries 8
```
**gtpp storage-server mode**

This command configures storage mode, local or remote, for CDRs. Local storage mode is available with ASR 5000 platforms only.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gtpp storage-server mode { local | remote | streaming }
default gtpp storage-server mode
```

- **default**
  Returns the GTPP group configuration to the default 'remote' value for the GTPP storage server mode.

- **local**
  Default: Disabled
  Specifies the use of the hard disk on the SMC for storing CDRs

  **Important:** This option is available with ASR 5000 platforms only.

- **remote**
  Specifies the use of an external server for storing CDRs. This is the default value.

- **streaming**
  Default: Disabled
  This keyword allows the operator to configure “streaming” mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:
  - When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.
  - If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF.

  **Important:** This option is available with ASR 5000 platforms only.

**Usage**

This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.
Example
The following command configures use of a hard disk for storing CDRs.

```
gtpp storage-server mode local
```
gtpp storage-server timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```gtpp storage-server timeout duration```
```
default gtpp storage-server timeout```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restores the timeout duration to the 30-second default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 30</td>
</tr>
<tr>
<td>Specifies the maximum amount of time the system waits for a response from the GTPP back-up storage server before assuming the packet is lost.</td>
</tr>
<tr>
<td><code>duration</code> is measured in seconds and can be configured to any integer value from 30 to 120.</td>
</tr>
</tbody>
</table>

Usage

This command works in conjunction with the `gtpp storage-server max-retries` command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of 60 seconds:

```
gtpp storage-server timeout 60```

gtpp suppress-cdrs zero-volume-and-duration

This command suppresses the CDRs created by session having zero duration and/or zero volume. By default this mode is ‘disabled’.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax


gtpp suppress-cdrs zero-volume-and-duration { gcdrs [ egcdrs ] | egcdrs [ gcdrs ] }

default gtpp suppress-cdrs zero-volume-and-duration

**default**
Disables the CDR suppression mode.

**gcdrs [ egcdrs ]**
Specifies that this command will handle G-CDRs before eG-CDRs.

**egcdrs [ gcdrs ]**
Specifies that this command will handle eG-CDRs before G-CDRs.

Usage
Use this command to suppress the CDRs (G-CDRs and eG-CDRs) which were created due with zero-duration session and zero-volume session due to any reason. By default this command is disabled and system will not suppress any CDR.

Example
The following command configures the system to suppression the eG-CDRs created for a zero duration session or zero volume session:

```
gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs
```
gtpp timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the CGF.

Product
GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtpp timeout time
default gtpp timeout
```

```
default
Resets the systems GTPP timeout value to 20 seconds.
```

```
time
Default: 20
Specifies the maximum amount of time the system waits for a response from the CGF before assuming the packet is lost.
time is measured in seconds and can be configured to any integer value from 1 to 60.
```

Usage
This command works in conjunction with the `gtpp max-retries` command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged. This parameter specifies the time between retries.

Example
The following command configures a retry timeout of 30 seconds:

```
gtpp timeout 30
```
gtpp trigger

This command disables GTTP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTTP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTTP trigger changes take affect immediately, except volume-limit.

Product
ECS, GGSN, SGSN

Privilege
Security Administrator, Administrator

Syntax


default gtpp trigger

default
Sets the specified trigger condition back to the default setting. All trigger conditions are enabled by default.

no
Re-enables the specified trigger condition.

cell-update
Enables the cell update trigger for S-CDRs, if the dictionary specified in the gtpp dictionary configuration includes support for cell update. This trigger is available only for 2G. Currently, custom18 dictionary supports the cell update trigger.

direct-tunnel
Enables the direct tunnel trigger for CDRs.

egcdr max-losdv
Default: Disabled
Enables the trigger for an eG-CDR if the List of Service Data Volume (LoSDV) containers crosses the configured limit for LOSDV containers.

inter-plmn-sgsn-change
This keyword is for GGSN only.
Default: Enabled
Disabling this trigger ignores an Inter-PLMN SGSN change and doesn't release a G-CDR.

ms-timezone-change
This keyword is specific to GGSN.
Default: Enabled
No partial record closure for a time zone change occurs when this trigger is disabled. MS Time zone change should be applicable only for 3GPP R6 based GTPP dictionaries.

plmn-id-change
This trigger keyword is specific to the 2G SGSN and is proprietary (non-standard).
Default: Disabled
Enables the PLMNID change trigger for S-CDRs if the dictionary specified in the gtpp dictionary configuration supports the PLMNID change. If enabled, the SGSN generates a partial S-CDR when the MS changes the PLMN while under the same SGSN (intra-system intra-SGSN PLMN-ID handover). Currently, custom18 dictionary supports this trigger.

qos-change
Default: Enabled
Enables the QoS-change trigger for CDRs. Disabling this trigger ignores a QoS-change and does not open a new CDR for it.

rat-change
Default: Enabled
This keyword enable/disable the partial record closure for a RAT change. If disabled no partial record closure for a RAT change occurs. RAT change should be applicable only for 3GPP R6 based GTPP dictionaries.
In SGSN, RAT change trigger (2G<->3G) means inter-service handoff (SGSN service <-> GPRS service). If this trigger is enabled, after the RAT change interim CDR is generated. After this RAT change CDR, CDR thresholds such as volume/time etc. and GTPP Group are applicable from new service. If RAT change trigger is disabled, the CDR thresholds and GTPP group etc. will not change and will continue to use from old service.
After the RAT change the System Type field in CDR changes to indicate the new system type. If this trigger is disabled then the next CDR generated will indicate System Type but the data count in the CDR does not necessarily belong to the system type indicated in CDR instead it may belong to both 2G and 3G as CDR is not closing when handover takes place.

Important: However System Type field in CDR related change is not applicable to customized CDR formats which does not use System Type field

routing-area-update
Enables the routing-area-update trigger for CDRs.

sgsn-change-limit [ also-intra-sgsn-multiple-address-group-change ]
This keyword is for GGSN only.
Default: Enabled
Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.
also-intra-sgsn-multiple-address-group-change : This keyword includes Intra-SGSN group changes as an SGSN change.

tariff-time-change
Default: Enabled
When this trigger is disabled container closure does not happen for a tariff-time change. This trigger is applicable for G-MB-CDRs for MBMS session too.
**time-limit**
Default: Enabled
When this trigger is disabled no partial record closure occurs when the configured time limit is reached.
This trigger is applicable for G-MB-CDRs for MBMS session too.

**volume-limit**
Default: Enabled
When this trigger is disabled no partial record closure occurs when volume limit is reached.
This trigger is applicable for G-MB-CDRs for MBMS session too.

**Usage**
Use this command to disable or re-enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

**Example**
The following command disables partial record closure when a configured time limit is reached:

```
gtp trigger time-limit
```

The following command re-enables partial record closure when a configured time limit is reached:

```
no gtp trigger time-limit
```
gtpp transport-layer

This commands selects the transport layer protocol for Ga interface for communication between AGW (GSNs) and GTPP servers.

**Product**
GGSN, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpp transport-layer { tcp | udp }
default gtpp transport-layer
```

---

**default**
Reset the transport layer protocol to GTPP servers to the default UDP.

---

**tcp**
Default: Disabled
Enables the system to implement TCP as transport layer protocol for communication with GTPP server.

---

**udp**
Default: Enabled
Enables the system to implement UDP as transport layer protocol for communication with GTPP server.

---

**Usage**
Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

---

**Example**
The following command enables TCP as the transport layer protocol for the GSN’s Ga interface.

```
gtpp transport-layer tcp
```
Chapter 115
GTP-U Service Configuration Mode Commands

The GTP-U Service Configuration Mode is used to manage parameters applied to incoming GTP-U packets.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          gtpu-service name
            GTP-U Service Configuration Mode
```
bind

Configures the IP address to use for GTP-U data packets.

Product
GGSN, P-GW, S-GW

Privilege
Administrator

Syntax

bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }

[ no ]

no

removes a configured IP address from this service.

bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }

Binds the service to an interface with an IPv4 address, IPv6 address or both.

ipv4-address ipv4_address [ ipv6-address ipv6_address ]: Binds this service to the IPv4 address of a configured interface. Optionally, bind the service to a configured interface with an IPv6 address. ipv4_address must be entered as a standard IPv4 address in dotted decimal notation.

ipv6-address ipv6_address [ ipv4-address ipv4_address ]: Binds this service to the IPv6 address of a configured interface. Optionally, bind the service to a configured interface with an IPv4 address. ipv6_address must be entered as a standard IPv6 address in colon-separated notation.

Usage

Use this command to bind the service to an interface for sending/receiving GTP-U packets.

Example

The following command configures the IPv4 address for this GTP-U service as 1.2.3.4:

bind ipv4-address 1.2.3.4
echo-interval

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-U echo packets are sent.

**Product**

GGSN, P-GW, S-GW

**Privilege**

Administrator

**Syntax**

```plaintext
echo-interval seconds
[ default | no ] echo-interval
```

- **default**
  Returns the command to its default setting of disabled.

- **no**
  Removes the configured echo-interval setting.

- **seconds**
  Specifies the number of seconds between the sending of a GTP-Uv1 echo packet. `seconds` must be an integer value from 60 to 3600.

**Usage**

Use this command to configure the rate at which GTP-Uv1 echo packets are sent.

**Example**

The following command sets the rate between the sending of echo packets at 120 seconds:

```plaintext
echo-interval 120
```
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
extention-header

Configures the addition of an extention header, in the GTP-U packet header, allowing for error indication messages.

Product
GGSN, P-GW, S-GW

Privilege
Administrator

Syntax

```
[ default | no ] extention-header source-udp-port
```

- **default**
  Returns the command to its default setting of disabled.

- **no**
  Disables the feature.

- **source-udp-port**
  Configures extension header type UDP Port support in GTP-U header for GTP-U Error Indication messages.

Usage

Example
The following command enables the inclusion of an extention header to allow for error indication messages:

```
extention-header source-udp-port
```
max-retransmissions

Configures the maximum retry limit for GTP-U echo retransmissions.

Product
GGSN, P-GW, S-GW

Privilege
Administrator

Syntax

max-retransmissions num

no max-retransmissions

no
Disables the feature.

num
Default: 4
Specifies the number of GTP-U echo message retransmissions allowed before triggering a path failure error condition. num must be an integer value from 0 to 15.

Usage
Use this command to set the maximum number of GTP-U echo message retransmissions in order to define a limit that triggers a path failure error.

Example
The following command sets the maximum GTP-U echo message retransmissions for this service to 10:
max-retransmissions 10
path-failure detection-policy

Configures a path failure detection policy on GTP-U echo messages that have been retransmitted the maximum number of retry times.

Product
GGSN, P-GW, S-GW

Privilege
Administrator

Syntax

path-failure detection-policy gtp echo

[ default | no ] path-failure detection-policy

- default
  Resets the command to its default setting of enabled.

- no
  Disables the feature.

- gtp echo
  Sets the detection policy to detect a failure upon reaching the maximum number of GTP-U echo message retransmissions.

Usage
Use this command to set the detection policy for path failures.

Example
The following command sets the path failure detection policy to detect failures upon reaching the maximum number of GTP-U echo message retries:

    path-failure detection-policy gtp echo
retransmission-timeout

Configures retransmission timeout for GTPU echo message retransmissions for this service.

Product
GGSN, P-GW, S-GW

Privilege
Administrator

Syntax

retransmission-timeout seconds

default retransmission-timeout

default
Returns the command to its default setting of 5.

seconds
Default: 5
Specifies the number of seconds between the re-sending of GTP-U echo messages. seconds must be an integer value between 1 and 20.

Usage
Use this command to set the number of seconds between the retransmission of GTP-U echo messages.

Example
The following command sets the number of seconds between the sending of GTP-U echo messages to 7:
retransmission-timeout 7
Chapter 116
HA Proxy DNS Configuration Mode Commands

The HA Proxy DNS Configuration Mode is used to create rules for HA proxy DNS intercept lists that redirect packets with unknown foreign DNS addresses to a home network DNS server.

**Important:** HA Proxy DNS Intercept is a license-enabled feature.

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

Exits the HA Proxy DNS Configuration Mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the HA Proxy DNS Configuration Mode and returns to the Context Configuration Mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

exit

**Usage**

Use this command to return to the Context Configuration Mode.
pass-thru

Sets IP addresses that should be allowed through the proxy DNS intercept feature.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] pass-thru ip_address [ /ip_mask ]
```

- **no**
  Removes the DNS IP address from the pass-thru rule.

```
pass-thru ip_address [ /ip_mask ]
```

Specifies an DNS IP address that is allowed through the intercept feature.

- `ip_address[/ip_mask]`: Specifies the IP address and network mask bits. `ip_address[/ip_mask]` is specified using the standard IPv4 or IPv6 dotted decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask (x.x.x.x/x).

**Usage**

Use this command to identify DNS IP addresses that should be allowed through the intercept feature. For a more detailed explanation of the proxy DNS intercept feature, see the `proxy-dns intercept-list` command in the Context Configuration Mode Commands chapter. A maximum of 16 intercept rules (either `redirect` or `pass-thru`) are allow for each intercept list.

**Important:** To allow packets through that do not match either the `pass-thru` or `redirect` rules, set a `pass-thru` rule address as: 0.0.0.0/0. If a packet does not match either the `pass-thru` or `redirect` rule, the packet is dropped.

**Example**

The following command allows a foreign network’s DNS with an IP address of 12.3.456.789 to avoid being redirected:

```
pass-thru 12.3.456.789
```
**redirect**

DNS IP addresses from foreign networks matching an IP address in this command are redirected to a home network DNS.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] redirect any [ primary-dns ip_address [ secondary-dns ip_address ] ]
```

- `no`
  Removes the DNS IP address from the redirect rule.

- `primary-dns ip_address`
  Specifies the IP address of the primary home network DNS. `ip_address` is specified using the standard IPv4 or IPv6 dotted decimal notation.

- `secondary-dns ip_address`
  Specifies the IP address of the secondary home network DNS. `ip_address` is specified using the standard IPv4 or IPv6 dotted decimal notation.

**Usage**

Use this command to identify DNS IP addresses from foreign networks that are to be redirected to the home DNS. For a more detailed explanation of the Proxy DNS feature, see the `proxy-dns intercept-list` command in the Context Configuration Mode Commands chapter. A maximum of 16 intercept rules (either `redirect` or `pass-thru`) are allowed for each intercept list.

Since this command is configured in the source context, the destination context containing the path to the home network DNS is identified using the Context Configuration Mode command `ip dns-proxy source-address`.

**i Important:** If a packet does not match the `pass-thru` or `redirect` rule, the packet is dropped. If `primary-dns` or `secondary-dns` is not configured, DNS messages are redirected to the primary-dns-server (or the secondary-dns-server) configured for the subscriber OR inside the context.

The following command identifies a foreign network DNS with an IP address of 1.23.456.789 and redirects it to a primary home network DNS with an IP address of 1.98.765.432:

```
redirect 1.23.456.789 primary-dns 1.98.765.432.
```
Chapter 117
HA Service Configuration Mode Commands

The Home Agent Service Configuration Mode is used to create and manage the Home Agent (HA) services associated with the current context.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

ha-service name

HA Service Configuration Mode
```
aaa

Configures the sending of subscriber session AAA accounting by the HA service.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

aaa accounting

no aaa accounting

Usage
Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers.
The chassis is shipped from the factory with the AAA accounting enabled.

Important: In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the aaa accounting subscriber radius command.

AAA accounting for the HA service can be disabled using the no version of the command.

Example
The following command disables aaa accounting for the HA service:

no aaa accounting
authentication

Configures authentication parameters for a specific HA service of a specific context.

**Product**
HA, ASN-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
authentication {aaa-distributed-mip-keys [ disabled | optional | required ] | dmu-refresh-key | imsi-auth | mn-aaa {allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth } | mn-ha { allow-noauth | always } }

no authentication {aaa-distributed-mip-keys required | imsi-auth }

default authentication [aaa-distributed-mip-keys | imsi-auth | mn-aaa | mn-ha ]
```

- **no**
  Disable the parameter.

- **default**
  Reset the specified option to its default setting.

- **aaa-distributed-mip-keys [ disabled | optional | required ]**
  Configures use of AAA distributed MIP keys for authenticating RRQ for WiMAX HA calls.
  Default is disabled.
  - **disabled**: Disables using AAA distributed WiMAX MIP keys for authenticating MIP RRQ.
  - **optional**: Use AAA distributed WiMAX MIP keys for authenticating RRQ with fallback option to use static/3GPP2 based MIP keys.
  - **required**: AAA distributed WiMAX MIP keys for authenticating MIP RRQ are mandatory

- **dmu-refresh-key**
  Typically, when a DMU resets then the next MIP re-registration causes MN-HA authorization failure and the HA rejects the MIP RRQ. This parameter enables the HA to retrieve the MN-HA key again from the AAA during the call and to use the freshly retrieved key value to recheck authentication.
  Default is disabled.

- **imsi-auth**
  Enable uses the IMSI to determine if MN-AAA or MN-FAC extensions are not present in the RRQ.
  Default is disabled.

- **mn-aaa { allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth }**
  Specifies how mobile node-to-AAA authentication extension in registration requests from the mobile node should be handled by the HA service.
Default is always.

**allow-noauth**: Specifies that the HA service does not require authentication for every mobile node registration request. However, if the mn-aaa extension is received, the HA service will authenticate it.

**always**: Specifies that the HA service will perform authentication each time a mobile node registers.

**dereg-noauth**: Disables authentication request upon de-registration.

**noauth**: Specifies that the HA service will not look for mn-aaa extension and will not authenticate it.

**renew-reg-noauth**: Specifies that the HA service will not perform authentication for mobile node re-registrations. Initial registration and de-registration will be handled normally.

**renew-and-dereg-noauth**: Disables authentication request upon re-registration and de-registration.

```
mn-ha { allow-noauth | always }
```

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ. Default is always.

**allow-noauth**: Allows a request that does not contain the auth extension.

**always**: A request should always contain the auth extension to be accepted.

**Usage**

The `authentication` command, combined with a keyword, can be used to specify how the system will perform authentication of registration request messages.

**Example**

The following command configures the HA service to always perform mobile node authentication for every registration request.

```
authentication mn-aaa always
```

The following command configures the HA service to always look for an MN-HA authentication extension in the RRQ.

```
authentication mn-ha always
```
bind

Binds the HA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

Product
HA

Privilege
Security Administrator, Administrator

Syntax
bind address address [max-subscribers count]

  no bind address

address
Specifies the IP address (address) of the interface configured as the Pi interface. address is specified in dotted decimal notation.

max-subscribers count
Default: 500000
Specifies the maximum number of subscribers that can access this service on this interface.

count can be configured to any integer value between 0 and 1,000,000.

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active PACs/PSCs installed in the system. A fully loaded system with 13 active PACs/PSCs can support 1,000,000 total subscribers. Refer to the license key command for additional information.

Usage
Associate the HA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the max-subscribers option, be sure to consider the following:

  ● The total number of interfaces that you will configuring for use as Pi interfaces

  ● The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours

  ● The average bandwidth for each of the sessions

  ● The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Use the no bind address command to delete a previously configured binding.
Example

The following command would bind the logical IP interface with the address of 192.168.3.1 to the HA service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```
binding-update

Configures MIP binding-update message related parameters.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
binding-update { max-retransmission num | retransmission-timeout seconds }
```

- **max-retransmission num**
  - Default 3.
  - Configures the number of times the message shall be transmitted. *num* must be an integer from 1 through 5.

- **retransmission-timeout seconds**
  - Default 2.
  - Configures the transmission timeout for the message in seconds. *seconds* must be an integer from 1 through 60.

Usage

Configure binding update parameters.

Example

Set the maximum number of times a MIP binding update message is transmitted to 4 with the following command:
```
binding-update max-retransmission 4
```
default

Restore default values assigned for specified parameter.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
default { authentication { imsi-auth | mn-aaa | mn-ha } | binding-update { max-retransmission | retransmission-timeout } | encapsulation { gre { checksum | checksum-verify | reorder-timeout | sequence-mode | sequence-numbers } | ip local-port | policy | null-username | nw-reachability-fail | overload | private-address allow-to-reverse-tunnel | reg-lifetime | reverse-tunnel | revocation { enable | max-retransmission | retransmission-timeout | trigger handoff | setup-timeout | simul-bindings } }
```

authentication

**imsi-auth**: Restores imsi-authentication to its default which is disabled.

**mn-aaa**: Restores the Foreign Agent (FA) mobile node re-registration authentication setting to its default: always.

**mn-ha**: Configures the HA service to it’s default behavior of looking for an MN-HA authentication extension in the RRQ.

**binding-update { max-retransmission | retransmission-timeout }**

Sets the MIP binding-update message related parameters to their defaults.

**max-retransmission**: Default 3.

Configures the number of times the message shall be transmitted to 3.

**retransmission-timeout**: Configures the transmission timeout for the message to 2 seconds.

**encapsulation**

Sets MIP data encapsulation using GRE to its default: enabled.

**gre { checksum | checksum-verify | reorder-timeout | sequence-mode | sequence-numbers }**

Sets default Generic Routing Encapsulation (GRE) parameters.

**checksum**: Disables the introduction of the checksum field in outgoing GRE packets.

**checksum-verify**: Disables verification of the GRE checksum (if present) in incoming GRE packets.

**reorder-timeout**: sets the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to the default setting: 100.

**sequence-mode**: Disables the reordering of incoming out-of-sequence GRE packets by setting this parameter to the default setting: none.

**sequence-numbers**: Disables the insertion or removal of GRE sequence numbers in GRE packets.

**ip local-port**

Restores the ip local-port setting to its default: 434.
policy (null-username | nw-reachability-fail | overload )
Restores the Home Agent service session policy settings.
null-username: Reject all RRQs that do not have an NAI.
nw-reachability-fail: If the network is not reachable, reject all incoming sessions.
overload: Restores the Home Agent service session overload policy setting to its default: reject.

private-address allow-no-reverse-tunnel
Reset the HA so that it does not accept MIP calls that use a private address without reverse tunneling.

reg-lifetime
Restores the Mobile IP session registration lifetime setting configured by the reg-lifetime command to its default: 600 seconds.

reverse-tunnel
Restores the reverse tunneling setting to its default: enabled.

revocation [ enable | max-retransmission | retransmission-timeout | trigger { handoff | idle-timeout} ]
Sets the MIP Registration Revocation settings to their default values. When no optional keywords are specified all revocation settings are set to their defaults.
enable: Disables MIP Registration Revocation on the FA.
max-retransmission: Sets the maximum number of retransmissions to 3.
retransmission-timeout: Sets the retransmission timeout to 3 seconds.
trigger { handoff | idle-timeout}: handoff enables inter-Access Gateway/FA handoff as a trigger for MIP Registration Revocation. idle-timeout enables session idle timer expiration as a trigger for MIP Registration Revocation.

setup-timeout
Restore the maximum amount of time allowed for setting up a session to the default: 60 seconds.

simul-bindings
Restores the simultaneous bindings setting to its default: 3.

Usage
After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

Example
The following command is used to return the ip local-port parameter to it’s default value:
default ip local-port
default subscriber

Specifies the name of a subscriber profile configured within the same context as the HA service from which to base the handling of all other subscriber sessions handled by the HA service.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
default subscriber profile_name
```

```
no default subscriber profile_name
```

(profile_name)

Specifies the name of the configured subscriber profile. profile_name can be between 1 and 63 alpha and/or number characters and is case sensitive.

Usage
Each subscriber profile specifies “rules” such as permissions, PPP settings, and timeout values. By default, the HA service will use the information configured for the subscriber named default within the same context. This command allows for multiple HA services within the same context to apply different “rules” to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the no default subscriber profile_name command to delete the configured default subscriber.

Example
To configure the HA service to apply the rules configured for a subscriber named user1 to every other subscriber session it processes, enter the following command:

```
default subscriber user1
```
encapsulation allow gre

Enables or disables the use of Generic Routing Encapsulation (GRE) when establishing a MIP (Mobile IP) session with an FA. When enabled, if requested by the FA, GRE encapsulation is used when establishing a Mobile IP (MIP) session. If disabled, when an FA requests GRE encapsulation, the HA denies the request.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
encapsulation allow { gre | keyless-gre }
no encapsulation allow { gre | keyless-gre }
```

```
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>gre</strong></td>
<td>Default: Enabled. Configures the use of GRE in Mobile IP session with an FA.</td>
</tr>
<tr>
<td><strong>keyless-gre</strong></td>
<td>Default: Disabled. Configures the GRE without key encapsulation in Mobile IP session with an FA.</td>
</tr>
</tbody>
</table>
```

Usage
Use to disable or re-enable the use of GRE encapsulation or Key-less encapsulation for MIP sessions. In case of chassis HA operating with other vendor equipment, which does not support the 3GPP2 to exchange key, this command with `keyless-gre` keyword will make the chassis HA to accept MIP data with legacy GRE.

Example
To disable GRE encapsulation for MIP sessions, enter the following command:
```
no encapsulation allow gre
```
To re-enable GRE encapsulation for MIP sessions, enter the following command:
```
encapsulation allow gre
```
To enable Key-less GRE encapsulation for MIP sessions, enter the following command:
```
encapsulation allow keyless-gre
```
end

Exits the HA service configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
end
```

Usage
Change the mode back to the Exec mode.
exit

Exits the HA service configuration mode and returns to the context configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
fa-ha-spi

Configures the security parameter index (SPI) between the HA service and the FA.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

fa-ha-spi remote-address fa_ip_address spi-number number { encrypted secret enc_secret | secret secret } [description string] [hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }] [replay-protection { timestamp | timestamp-tolerance | nonce }] +
no fa-ha-spi remote-address ha_ip_address spi-number number

remote-address fa_ip_address

Specifies the IP address of the FA. fa_ip_address is an IP address or an IP address and mask expressed in dotted decimal notation.

Important: The system supports unlimited peer FA addresses per HA but only maintains statistics for a maximum of 8192 peer FAs. If more than 8192 FAs are attached, older statistics are identified and overwritten.

spi-number number

Specifies the SPI (number) which indicates a security context between the FA and the HA in accordance with RFC 2002.

number can be configured to any integer value between 256 and 4294967295.

encrypted secret enc_secret | secret secret

Configures the shared-secret between the HA service and the FA. The secret can be either encrypted or non-encrypted.

encrypted secret enc_secret: Specifies the encrypted shared key (enc_secret) between the HA service and the FA. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.

secret secret: Specifies the shared key (secret) between the HA service and the FA. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

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

description string

This is a description for the SPI. string must be an alpha and or numeric string of from 1 through 31 characters.

hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5
Specifies the hash-algorithm used between the HA service and the FA.

`hmac-md5`: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
`md5`: Configures the hash-algorithm to implement MD5 per RFC 1321.
`rfc2002-md5`: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

```
replay-protection { timestamp [timestamp-tolerance tolerance] | nonce }
```

Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.

- `nonce`: Configures replay protection to be implemented using NONCE per RFC 2002.
- `timestamp`: Configures replay protection to be implemented using timestamps per RFC 2002.
- `timestamp-tolerance`: Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. `tolerance` is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 60.

```
traffic-group grp_num
```

The traffic-group attribute is meant to tag the remote FA so that traffic policy can be enforced according to the traffic-group value. This attribute can be used by ECS to handle subscriber traffic coming from FAs with a specified traffic group differently.

Note: the functionality controlled by this keyword is only available if a License for Content Access Control has been purchased and enabled.

`grp_num` must be an integer from 1 through 255.

More than one of the above keywords can be entered within a single command.

---

**Usage**

An SPI is a security mechanism configured and shared by the HA service and the FA. Please refer to RFC 2002 for additional information.

Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a “default” SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.

---

**Important:** The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2048 SPIs can be configured per HA service.

Use the `no` version of this command to delete a previously configured SPI.

---

**Example**

The following command configures the FA service to use an SPI of 512 when communicating with an HA with the IP address 192.168.0.2. The key that would be shared between the HA and the FA service is q397F65. When communicating with this HA, the FA service will also be configured to use the rfc2002-md5 hash-algorithm.

```
fa-ha-spi remote-address 192.168.0.2 spi-number 512 secret q397F65 hash-algorithm rfc2002-md5
```

The following command deletes the configured SPI of 400 for an HA with an IP address of 172.100.3.200:

```
no fa-ha-spi remote-address 172.100.3.200 spi-number 400
```
gre

Configures Generic Routing Encapsulation (GRE) parameters.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
gre { checksum | checksum-verify | reorder-timeout timeout | sequence-mode { none | reorder } | sequence-numbers }
```

no gre { checksum | checksum-verify | sequence-numbers }

Disables the specified functionality.

**checksum**

Default: disabled

Enables the introduction of the checksum field in outgoing GRE packets.

**checksum-verify**

Default: disabled

Enables verification of the GRE checksum (if present) in incoming GRE packets.

**reorder-timeout timeout**

Default: 100

Configures maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. `timeout` must be an integer from 0 through 5000.

**sequence-mode { none | reorder }**

Default: none

Configures how incoming out-of-sequence GRE packets should be handled.

- **none**: Disables reordering of incoming out-of-sequence GRE packets.
- **reorder**: Enables reordering of incoming out-of-sequence GRE packets.

**sequence-numbers**

Default: Disabled

Enables the insertion of sequence numbers into the GRE packets.

**Usage**

Use this command to configure how the HA service handles GRE packets.

**Example**

To set maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to 500 milliseconds, enter the following command:
gre reorder-timeout 500
To enable the reordering of incoming out of sequence GRE packets, enter the following command:
gre sequence-mode reorder
To enable the insertion or removal of GRE sequence numbers in GRE packets, enter the following command:
gre sequence-numbers
idle-timeout-mode

Configures the method the HA service uses to determine when to reset a session idle timer.

**Product**  
HA

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
idle-timeout-mode { aggressive | handoff | normal } [ upstream-only ]
default idle-timeout-mode
```

**default**  
Reset the idle timeout mode to the default settings.  
Defaults: aggressive, upstream-only is disabled.

**aggressive**  
The session idle timer is reset only when MIP user data is detected. This is the default behavior.

**handoff**  
The session idle timer is reset when MIP user data is detected and when an inter-Access Gateway/FA handoff occurs.

**normal**  
The session idle timer is reset when MIP user data is detected and when any MIP control signaling occurs.

**upstream-only**  
Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.

**Usage**

Use this command to set how the current HA service resets the idle timer for a session.

**Example**

To reset the idle timer whenever user data is detected or whenever an inter-Access Gateway/FA occurs, use the following command:

```
idle-timeout-mode handoff
```
**ip context-name**

Specifies name of the destination context to be applied to the subscribers; this would take precedence over the same in subscriber configuration and RADIUS return attributes.

This new configuration overrides the local subscriber configuration as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this particular destination context and IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip context-name name
```

**name**

Specifies the name of the context to assign the subscriber to once authenticated. name must be from 1 to 79 alpha and/or numeric characters.

**no**

**Usage**

Removes the current assigned context from the subscriber’s data. Set the name of the destination context to be applied to the subscribers.

**Example**

```
ip context-name sampleName
no ip context-name sampleName
```
ip local-port

Configures the local User Datagram Protocol (UDP) port for the Pi interfaces’ IP socket on which to listen for MOBILE IP Registration messages.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
ip local-port number
```

`number`

Specifies the UDP port number.
`number` can be any integer value between 1 and 65535.

Usage
Specify the UDP port that should be used for communications between the FA service and the HA. The chassis is shipped from the factory with the local port set to 434.

Example
The following command specifies a UDP port of 3950 for the HA service to use to communicate with the HA on the Pi interface:

```
ip local-port 3950
```
ip pool

Specifies name of the IP address pool or group to use for subscriber IP address allocation; this takes precedence over the same in subscriber configuration and RADIUS return attributes.

This new configuration overrides the local subscriber configuration as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this particular destination context and IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

ip pool name

- name
  Specifies the logical name of the IP address pool. name must be from 1 to 31 alpha and/or numeric characters.

- no
  Indicates the IP address pool specified is to be removed from the current context’s configuration or disable the specified option for an IP pool.

Usage
Define a pool of IP addresses for the context to use in assigning IPs for this service.

Example

ip pool pool1
no ip pool pool1
isakmp

Configures the crypto map for a peer HA and configures the default crypto map for the FA service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
isakmp { peer-fa fa_address | skew-lifetime time | aaa-context context_name }
```

no

Deletes the reference to the crypto map for the specified HA, deletes the reference for the default crypto map, resets the skew-lifetime to the default, or resets the aaa-context to the default.

```
peer-fa fa_address { crypto map map_name [[ encrypted ] secret secret ]}
```

Configures a crypto map for a peer FA.

- **fa_address**: IP address of the peer FA to which this IPSEC SA will be established.
- **crypto map map_name**: The name of a crypto map configured in the same context that defines the IPSEC tunnel properties. `map_name` is the name of the crypto map and can be from 1 to 127 alpha and/or numeric characters.
- **encrypted**: This keyword is intended only for use by the chassis while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `secret` keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- **secret secret**: The pre-shared secret that will be used to during the IKE negotiation. `secret` is the secret string and can be from 1 to 127 alpha and/or numeric characters.

```
skew-lifetime time
```

Default: 10 seconds

Configures the IKE pre-shared key’s time skew.

`time` is the amount of time the IKE S key fetched from AAA is considered valid after the key has expired. It is measured in seconds and can be configured to any integer value from 1 to 65535.

```
aaa-context context_name
```

Default: The context in which the service is configured

Configures the name of the context on the system in which AAA functionality is performed. `context_name` is the name of the context through which the HA service accesses the HAAA server to fetch the IKE S Key and S Lifetime parameters. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.

**Usage**

Use this command to configure the FA-service’s per-HA IPSEC parameters. These dictate how the HA service is to establish an IPsec SA with the specified FA.
| HA Service Configuration Mode Commands |

**Important:** For maximum security, it is recommended that the above command be executed for every possible FA that the HA service communicates with.

Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

**Example**
The following command creates a reference for an HA with the IP address 1.2.3.4 to a crypto map named map1:

```
isakmppeer-fa 1.2.3.4 crypto map map1
```

The following command deletes the crypto map reference for the HA with the IP address 1.2.3.4.

```
o isakmppeer-fa 1.2.3.4
```

The following command sets the time an S key can used after the S lifetime expires to 120 seconds.

```
isakmp skew-lifetime 120
```

The following command creates the default reference for an HA to a crypto map named `map1`, where peer address is unknown:

```
isakmp default crypto map map1
```
mn-ha-spi

Configures the security parameter index (SPI) between the HA service and the mobile node.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
mn-ha-spi spi-number number [description string] [encrypted secret enc_secret | secret secret] [hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }] [permit-any-hash-algorithm] [replay-protection { nonce | timestamp }] [timestamp-tolerance tolerance]
```

```
no mn-ha-spi spi-number number
```

`spi-number number`

Specifies the SPI (number) which indicates a security context between the mobile node and the HA service in accordance with RFC 2002. number can be configured to any integer value between 256 and 4294967295.

`description string`

This is a description for the SPI. string must be an alpha and or numeric string of from 1 through 31 characters.

`encrypted secret enc_secret | secret secret`

Configures the shared-secret between the HA service and the mobile node. The secret can be either encrypted or non-encrypted.

- `encrypted secret enc_secret`: Specifies the encrypted shared key (enc_secret) between the HA service and the mobile node. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.
- `secret secret`: Specifies the shared key (secret) between the HA service and the mobile node. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

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

`hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5

Specifies the hash-algorithm used between the HA service and the mobile node.

- `hmac-md5`: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
- `md5`: Configures the hash-algorithm to implement MD5 per RFC 1321.
- `rfc2002-md5`: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

`permit-any-hash-algorithm`

Default: disabled
HA Service Configuration Mode Commands

Allows verification of the MN-HA authenticator using all other hash-algorithms after failure with configured hash-algorithm. Successful algorithm is logged to aid in troubleshooting and is used to create the MN-HA authenticator in the Registration Reply message.

```
replay-protection { nonce | timestamp }
```
Default: timestamp
Specify the replay-protection scheme that should be implemented by the HA service for this SPI.
- `nonce`: configures replay protection to be implemented using NONCE per RFC 2002.
- `timestamp`: configures replay protection to be implemented using timestamps per RFC 2002.

```
timestamp-tolerance tolerance
```
Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.
Tolerance is measured in seconds and can be configured to any integer value between 0 and 65535.

Usage
An SPI is a security mechanism configured and shared by the HA service and the mobile node. Please refer to RFC 2002 for additional information.
Use the no version of this command to delete a previously configured SPI.

Example
The following command configures the HA service to use an SPI of 640 when communicating with a mobile node. The key that would be shared between the mobile node and the HA service is q397F65.

```
mn-ha-spi spi-number 640 secret q397F65
```
The following command deletes the configured SPI of 400:
```
no mn-ha-spi spi-number 400
```
**nat-traversal**

This command enables NAT traversal and also configures the forcing of UDP tunnels for NAT traversal.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
nat-traversal [force-accept]
no nat-traversal [force-accept]
default nat-traversal [force-accept]
```

**no**
Disables NAT traversal or disables forcing the acceptance of UDP tunnels for NAT traversal.

**default**
Reset the defaults for this command.
Default: NAT traversal disabled, force-accept disabled.

**force-accept**
This keyword configures the HA to accept requests when NAT is not detected but the Force (F) bit is set in the RRQ with the UDP Tunnel Request. By default this type of request is rejected if NAT is not detected.

**Usage**
Use this command to enable NAT traversal and enable the forcing of UDP tunnels for NAT traversal.

**Example**
The following command enables NAT traversal for the current HA service and forces the HA to accept UDP tunnels for NAT traversal:

```
nat-traversal force-accept
```
**optimize tunnel-reassembly**

Configures HA to FA optimization for tunnel reassembly.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
optimize tunnel-reassembly

no optimize tunnel-reassembly
```

**Usage**

Enabling this functionality fragments large packets prior to encapsulation for easier processing.

Tunnel reassembly optimization is disabled by default.

**Important:** Cisco Systems strongly recommends that you do not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

**Important:** This functionality works best when the HA service is communicating with an FA service running in a system. However, an HA service running in the system communicating with an FA from a different manufacturer will operate correctly even if this parameter is enabled.

Use the `no` version of this command to disable tunnel optimization if enabled.

**Example**

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```
**policy bc-query-result**

Configures the response code to send in a binding cache (BC) query result in response to a network failure or error.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
policy bc-query-result network-failure code
[ default ] policy bc-query-result network-failure
```

- **network-failure code**
  Default: 0xFFFF
  Specify the response code for BC responses sent on network failures.
  `code` must be either 0xFFFF or 0xFFFE.

**Usage**
Use this command to specify the type of response code to send in a P-MIP BC query result.

**Example**
The following command sets the P-MIP BC query result response code to 0xFFFE:
```
policy bc-query-result network-failure 0xFFFE
```
**policy nw-reachability-fail**

Specifies the action to take upon detection of an up-stream network-reachability failure.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
policy nw-reachability-fail { reject [use-reject-code { admin-prohibited | insufficient-resources } ] | redirect ip_addr1 [weight value] [ip_addr2 [weight value] ... ip_addr16 [weight value]] }
nopoly nw-reachability-fail [redirect ip_addr1 ... ip_addr16]
```

**Usage**

Use this command to set the action for the HA service to take upon a network reachability failure.
**Important:** Refer to the context configuration mode command `nw-reachability server` to configure network reachability servers.

**Important:** Refer to the subscriber configuration mode command `nw-reachability-server` to bind the network reachability to a specific subscriber.

**Important:** Refer to the `nw-reachability server server_name` keyword of the context configuration mode `ip pool` command bind the network reachability server to an IP pool.

**Example**

To set the HA service to reject all new calls on a network reachability failure, enter the following command:

```
policy nw-reachability-fail reject
```

Use the following command to set the HA service to redirect all calls to the HA at IP address 192.168.100.10 and 192.168.200.10 on a network reachability failure:

```
policy nw-reachability-fail redirect 192.168.100.10 192.168.200.10
```
policy overload

Configures the overload policy within the HA service.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
policy overload { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }

no policy overload [ redirect address [ address2 ... address16 ] ]
```

Deleted previously set policy or removes a redirect IP address.

overload: This keyword without any options deletes the complete overload policy from the PDSN service.

overload redirect address [ address2 ... address16 ]; deletes up to 16 IP addresses from the overload redirect policy. The IP addresses must be expressed in IP v4 dotted decimal notation.

```
redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ]
```

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HA service rejects new sessions with a Registration Reply Code of 136H (unknown home agent address) and provides the IP address of an alternate HA. This command can be issued multiple times.

address: The IP address of an alternate HA expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

```
weight weight_num: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.
```

```
reject [ use-reject-code { admin-prohibited | insufficient-resources } ]
```

This option causes any overload traffic to be rejected. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).

```
use-reject-code { admin-prohibited | insufficient-resources } : Use the specified reject code when rejecting traffic.
```

```
admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.
```

```
insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.
```

Usage
The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system. The system automatically invokes the overload policy when an on-line software upgrade is started. Use the **no** version of this command to restore the default policy. The setting for overload policy is reject.

**Example**
The following command enables an overload redirect policy for the HA service that will send overload calls to either of two destinations with weights of 1 and 10 respectively:

```
policy overload redirect 192.168.100.10 weight 1 192.168.100.20 weight 10
```
policy null-username

Configures the current HA service to accept or reject an RRQ without an NAI extension.

**Important:** This command is customer specific and is license enabled.

**Product:**
HA

**Privilege:**
Security Administrator, Administrator

**Syntax**

```
policy null-username { accept-static | reject }
no policy null-username
```

**no**
Set the HA back to the default behavior of rejecting an RRQ without an NAI extension.

**accept-static**
This enable the HA to accept an RRQ with a static (i.e, non-zero) home address request but without NAI extension, when MN-AAA authentication is disabled at the HA. MN-NAI is required for MN-AAA authentication.

**reject**
Default. This is the default behavior of rejecting an RRQ without an NAI extension.

**Usage**
Use this command to enable or disable the HA from accepting an RRQ without an NAI.

**Example**
The following command enables the current HA service to accept RRQs that do not have an NAI extension:

```
policy null-username accept-static
```
private-address allow-no-reverse-tunnel

This command allows the HA service to accept private addresses without using reverse tunneling.

**Important:** This command is customer specific and is license enabled.

**Product**  
HA

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
private-address allow-no-reverse-tunnel
no private-address allow-no-reverse-tunnel

no
```

Reject MIP calls that use private addresses and do not use reverse tunneling.

**Usage**

Use this command to enable or disable the HA from accepting calls that use private addresses without reverse tunneling.

**Example**

The following command enables the current HA service to accept MIP calls that use private addresses but do not use reverse tunneling:

```
private-address allow-no-reverse-tunnel
```
**reg-lifetime**

Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```text
reg-lifetime time
no reg-lifetime
```

- **no**
  Sets the registration lifetime to infinite.

- **time**
  Specifies the registration lifetime.
  time is measured in seconds and can be configured to any integer value between 1 and 65534.

**Usage**

Use to limit a mobile node's lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply.

The chassis is shipped from the factory with the registration lifetime set to 600 seconds.

**Example**

The following command configures the registration lifetime for the HA service to be 2400 seconds:

```text
reg-lifetime 2400
```

The following command configures an infinite registration lifetime for MIP calls:

```text
no reg-lifetime
```
reverse-tunnel

Enables the use of reverse tunneling for a Mobile IP sessions when requested by the mobile node.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
reverse-tunnel

no reverse-tunnel
```

**Usage**
Reverse tunneling involves tunneling datagrams originated by the mobile node to the HA service via the FA. When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

Among the advantages of using reverse-tunneling are that:
- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Use the `no` version of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, triangular routing will be performed. Routing will be used.

The chassis is shipped from the factory with the reverse tunnel enabled.

**Important:** If reverse tunneling is disabled on the system and a mobile node requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

**Example**
The following command disables reverse-tunneling support for the HA service:

```plaintext
no reverse-tunnel
```
revocation

Enables the MIP revocation feature and configures revocation parameters.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
revocation { enable | max-retransmission number | negotiate-i-bit | retransmission-timeout secs | send-nai-ext | trigger { handoff | idle-timeout } }
```

```
o revocation | enable | negotiate-i-bit | send-nai-ext | trigger { handoff | idle-timeout }
```

**no**

Completely disables registration revocation on the HA, disables trigger handoff, or disables revocation on idle timer expiration.

**enable**

Enables the MIP registration revocation feature on the HA. When enabled, if revocation is negotiated with an FA and a MIP binding is terminated, the HA can send a Revocation message to the FA. This feature is disabled by default.

**max-retransmission number**

Default: 3
The maximum number of retransmissions of a Revocation message before the revocation fails. `number` must be an integer from 0 through 10.

**negotiate-i-bit**

Default: disabled
Enables the HA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

**retransmission-timeout secs**

Default: 3
The number of seconds to wait for a Revocation Acknowledgement from the FA before retransmitting the Revocation message. `secs` must be an integer from 1 through 10.

**send-nai-ext**

Default: off
Enables sending the NAI extension in the revocation message.

**trigger { handoff | idle-timeout }**

**handoff:** Default: Enabled
Triggers the HA to send a Revocation message to the FA when an inter-Access Gateway/FA handoff of the MIP session occurs. If this is disabled, the HA is never triggered to send a Revocation message.

**idle-timeout**: Default: Enabled

Triggers the HA to send a Revocation message to the FA when a session idle timer expires.

---

### Usage

Use this command to enable or disable the MIP revocation feature on the HA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

---

### Example

The following command enables Registration Revocation on the HA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 10:

```
revocation max-retransmission 10
```

The following command sets the timeout between retransmissions to 3:

```
revocation retransmission-timeout 3
```

The behavior of send MIP revocation to FA is as follows:

1. **1st retry**: Retransmit in 3 seconds after previous MIP revocation send.
2. **2nd retry**: Retransmit in 6 seconds after previous MIP revocation send (9 seconds after sending initial MIP revocation).
3. **3rd retry**: Retransmit in 12 seconds after previous MIP revocation send (21 seconds after sending initial MIP revocation).
4. **4th retry**: Retransmit in 24 seconds after previous MIP revocation send (45 seconds after sending initial MIP revocation).
5. **5th retry**: Retransmit in 48 seconds after previous MIP revocation send (93 seconds after sending initial MIP revocation).

---

**Important**: The value of retransmission-timeout doubles. HA disconnects the session forcibly in 120 seconds after sending initial MIP revocation.
setup-timeout

The maximum amount of time allowed for session setup.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

setup-timeout seconds

seconds
Default: 60 seconds
The maximum amount of time, in seconds, to allow for setup of a session. must be an integer from 1 through 1000000

Usage
Use this command to set the maximum amount of time allowed for setting up a session.

Example
To set the maximum time allowed for setting up a session to 5 minutes (300 seconds), enter the following command:
setup-timeout 300
simul-bindings

Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
simul-bindings number
```

`number`

Configures the maximum number of simultaneous “care-of” bindings that the HA service will maintain for any given subscriber. The number can be configured to any integer value between 1 and 5.

Usage
Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address. Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintains previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested. The chassis is shipped from the factory with the simultaneous sessions set to 3.

Example
The following command configures the HA service to support up to 4 MBRs per subscriber:

```
simul-bindings 4
```
threshold init-rrq-rcvd-rate

Set an alarm or alert based on the average number of calls setup per second for the context.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold init-rrq-rcvd-rate
```

```
no
```

Deletes the alert or alarm.

```
high_thresh
```

Default: 0
The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 1000000.

```
clear low_thresh
```

Default: 0
The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second > High Threshold
- **Clear condition:** Actual number of calls setup per second ≤ Low Threshold

Example

The following command configures a number of calls setup per second threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```
threshold ipsec-call-req-rej

Configures a threshold for the total IPSec calls request rejected.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold ipsec-call-req-rej high_thresh [ clear low_thresh ]

no threshold ipsec-call-req-rej
```

- **high_thresh**
  - Default: 0
  - The high threshold number of IPSec call requests rejected per second must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` can be configured to any integer value between 0 and 100000.

- **clear low_thresh**
  - Default: 0
  - The low threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to clear an alert or alarm.
  - `low_thresh` can be configured to any integer value between 0 and 100000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec call requests rejected is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition:** Actual number of IPSec IKE requests > High Threshold
- **Clear condition:** Actual number of IPSec IKE requests ≤ Low Threshold

**Example**

The following command configures a number of IPSec call requests rejected threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-call-req-rej 1000 clear 800
```
threshold ipsec-ike-failrate

Configures a threshold for the percentage of IPSec IKE failures.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
threshold ipsec-ike-failrate high_thresh [ clear low_thresh ]
```

no threshold ipsec-ike-failrate

no

Deletes the alert or alarm.

```
high_thresh
```

Default: 0

The high threshold percentage of IPSec IKE failures per second must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` can be configured to any integer value between 0 and 100.

```
clear low_thresh
```

Default: 0

The low threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.

`low_thresh` can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the percentage of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the percentage of IPSec IKE failures on the following rules:

- **Enter condition:** Percentage of IPSec IKE failures > High Threshold
- **Clear condition:** Percentage of IPSec IKE failures £ Low Threshold

Example

The following command configures a percentage of IPSec IKE failures threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

threshold ipsec-ike-failrate 90 clear 80
threshold ipsec-ike-requests

Configures a threshold for the total IPSec IKE failures.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold ipsec-ike-failures high_thresh [ clear low_thresh ]
```

```
no threshold ipsec-ike-failures
```

```
no
```

Deletes the alert or alarm.

```
high_thresh
```

Default: 0
The high threshold number of IPSec IKE failures per second must be met or exceeded within the polling interval to generate an alert or alarm.

```
high_thresh can be configured to any integer value between 0 and 100000.
```

```
clear low_thresh
```

Default: 0
The low threshold number of call IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.

```
low_thresh can be configured to any integer value between 0 and 100000.
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec IKE failures is equal to or greater than a specified number per second.
Alerts or alarms are triggered for the number of IPSec IKE failures on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures > High Threshold
- **Clear condition:** Actual number of IPSec IKE failures ≤ Low Threshold

**Example**
The following command configures a number of IPSec IKE failures threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:
```
threshold ipsec-ike-failures 1000 clear 800
```
threshold ipsec-ike-requests

Configures a threshold for the total IPSec IKE failures.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
threshold ipsec-ike-failures high_thresh [ clear low_thresh ]

no threshold ipsec-ike-failures
```

<table>
<thead>
<tr>
<th>no threshold ipsec-ike-failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes the alert or alarm.</td>
</tr>
</tbody>
</table>

```
high_thresh
```

| Default: 0 |
| The high threshold number of IPSec IKE failures per second must be met or exceeded within the polling interval to generate an alert or alarm. |

```
low_thresh
```

| Default: 0 |
| The low threshold number of call IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm. |

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE failures on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures > High Threshold
- **Clear condition:** Actual number of IPSec IKE failures ≤ Low Threshold

**Example**

The following command configures a number of IPSec IKE failures threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failures 1000 clear 800
```
threshold ipsec-tunnels-established

Configures a threshold for the total IPSec tunnels established.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
threshold ipsec-tunnels-established high_thresh [ clear low_thresh ]
```

```
no threshold ipsec-tunnels-established
```

`no`

Deletes the alert or alarm.

`high_thresh`

Default: 0

The high threshold number of IPSec tunnels established per second must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* can be configured to any integer value between 0 and 1000000.

`clear low_thresh`

Default: 0

The low threshold number of call IPSec tunnels established per second that must be met or exceeded within the polling interval to clear an alert or alarm.

*low_thresh* can be configured to any integer value between 0 and 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec tunnels established is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels established on the following rules:

- **Enter condition:** Actual number of IPSec tunnels established > High Threshold
- **Clear condition:** Actual number of IPSec tunnels established £ Low Threshold

**Example**

The following command configures a number of IPSec tunnels established threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-established 1000 clear 800
```
**threshold ipsec-tunnels-setup**

Configures a threshold for the total IPSec tunnels setup.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold ipsec-tunnels-setup high_thresh [ clear low_thresh ]

no threshold ipsec-tunnels-setup
```

**no**

Deletes the alert or alarm.

**high_thresh**

Default: 0
The high threshold number of IPSec tunnels setup per second must be met or exceeded within the polling interval to generate an alert or alarm.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**clear low_thresh**

Default: 0
The low threshold number of call IPSec tunnels setup per second that must be met or exceeded within the polling interval to clear an alert or alarm.

```
low_thresh can be configured to any integer value between 0 and 1000000.
```

**Usage**

Use this command to set an alert or an alarm when the number of IPSec tunnels setup is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels setup on the following rules:

- **Enter condition:** Actual number of IPSec tunnels setup > High Threshold
- **Clear condition:** Actual number of IPSec tunnels setup £ Low Threshold

**Example**

The following command configures a number of IPSec tunnels setup threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-setup 1000 clear 800
```
threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per HA service.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
threshold reg-reply-error high_thresh [ clear low_thresh ]
no threshold reg-reply-error
```

no
Deletes the alert or alarm.

```
high_thresh
```
Default: 0
The high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

```
clear low_thresh
```
Default: 0
The low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

⚠️ Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of registration reply errors on the following rules:
- **Enter condition:** Actual number of registration reply errors > High Threshold
- **Clear condition:** Actual number of registration reply errors £ Low Threshold

Example
The following command configures a registration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:
```
threshold reg-reply-error 1000 clear 500
```
threshold rereg-reply-error

Set an alarm or alert based on the number of re-registration reply errors per HA service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold rereg-reply-error high_thresh [ clear low_thresh ]
no threshold rereg-reply-error
```

*no*

Deletes the alert or alarm.

*high_thresh*

Default: 0

The high threshold number of re-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 1000000.

*clear low_thresh*

Default: 0

The low threshold number of re-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of re-registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of re-registration reply errors on the following rules:

- **Enter condition:** Actual number of re-registration reply errors > High Threshold
- **Clear condition:** Actual number of re-registration reply errors ≤ Low Threshold

**Example**

The following command configures a re-registration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold rereg-reply-error 1000 clear 500
```
threshold dereg-reply-error

Set an alarm or alert based on the number of de-registration reply errors per HA service.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
threshold dereg-reply-error high_thresh [ clear low_thresh ]
no threshold dereg-reply-error
```

**no**

Deletes the alert or alarm.

**high_thresh**

Default: 0
The high threshold number of de-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**clear low_thresh**

Default: 0
The low threshold number of de-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of de-registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of de-registration reply errors on the following rules:

- **Enter condition:** Actual number of de-registration reply errors > High Threshold
- **Clear condition:** Actual number of de-registration reply errors £ Low Threshold

**Example**

The following command configures a de-registration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```
wimax-3gpp2 interworking

Configures the interworking between WiMAX and 3GPP2 network at HA. This support provides handoff capabilities from 4G to 3G (PDSN) network access and vice-versa.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

[no | default] wimax-3gpp2 interworking

no
Disables the pre-configured interworking between WiMAX and 3GPP2 networks at HA level.

default
Configures the WiMAX-3GPP2 interworking to default setting; i.e. disabled.

Usage
Use this command to enable/disable the interworking between WiMAX and 3GPP2 network for seamless session continuity.
This functionality provides HA support for both 4G and 3G technology HA (WiMAX HA and PDSN/HA) for handoff from 4G and 3G network access (ASN GW/FA and PDSN/FA) and vice-versa.

Important: Use this command in conjunction with authentication aaa-distributed-mip-keys required command.

Example
The following command enables the interworking for a subscriber between WiMAX and 3GPP2 network.

wimax-3gpp2 interworking
Chapter 118
HD RAID Configuration Mode Commands

This mode develops default policies designed to minimize administrative intervention when setting up a RAID on ASR 5000 SMC hard disks.
default

Sets or restores the default condition for the selected parameter

Product

All

Privilege

Security Administrator, Administrator

Syntax

default ( overwrite { invalid | unknown | valid } disk | select )

overwrite { invalid | unknown | valid } disk
Confirms the system to overwrite any of the disk types

select
Selects the newer of the valid RAID disks when two valid RAID disks are available.

Usage

Selects default parameters

Example

Use the following example to select the newest disk in an SMC pair:

default select
end

Exits the HD RAID configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the HD RAID configuration mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
overwrite

Sets the RAID overwrite properties.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no | default ] overwrite { invalid | unknown | valid } disk [ -noconfirm ]

no
Prevents a disk from being overwritten.

default
Configures the default overwrite action:

invalid
This option allows the system to automatically overwrite invalid disks including empty disks, wrongly partitioned disks, and partially constructed disks.
This is the default overwrite action.

unknown
This option allows the system to automatically overwrite unknown disks that has a valid RAID superblock but is not configured in the standard way; most likely because it has data from a different version.

valid
This option allows the system to automatically overwrite a disk that is a clean RAID component but not part of the current or selected RAID.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Sets a policy for automatically overwriting different disk types. If there is a disk that satisfies the changed overwrite policy then the disk would overwrite immediately.

Example
The following command configures a policy for overwriting invalid RAID disks:

overwrite invalid disk -noconfirm
select

Configures the disk preference when both hard disks on the ASR 5000 have valid RAID information.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ default ] select { newer | none } disk [ -noconfirm ]

- **default**
  Configures the command to its default condition.

- **newer**
  Selects the newer disk by timestamp and event counter in superblocks. If all are the same, then the same array will start with both SMC disks, but a different array will need admin intervention).

- **none**
  Does not select any disk but defers to administrator intervention.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage
Determines the selected disc when two valid disks from either the same or different RAIDs are running on the ASR 5000.

Example
This command forces the RAID to be configured on the newer SMC hard disk:

```
select newer disk -noconfirm
```
The HD Storage Policy Configuration Mode is used to configure directory name and file parameters for Diameter record files being stored on the HD storage device.
**directory**

Configures the name of the directory on the HD storage drive where Diameter records are stored.

**Product**

HSGW, P-GW, S-GW

**Privilege**

Administrator

**Syntax**

`directory name dir_name`

`default directory name`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>directory</code></td>
<td>Configures the name of the directory on the HD storage drive where Diameter records are stored.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Returns the command to its default setting of using the policy name as the directory name.</td>
</tr>
<tr>
<td><code>name dir_name</code></td>
<td>Specifies the name to be applied to the directory. <code>dir_name</code> must be an alpha and or numeric string from 1 to 63 characters. When configured, the actual directory path is: <code>/hd-raid/records/&lt;record-type&gt;/&lt;dir_name&gt;/</code>. So if the directory name variable is entered as &quot;sgwpgw&quot;, the path is: <code>/hd-raid/records/acr/sgwpgw</code>.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to name a directory on the HD storage drive where Diameter records are to be stored.

**Example**

The following command configures a directory named `cdr1`:

`directory name cdr1`
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
file

Configures file parameters for Diameter records being stored on the HD storage device.

Product
HSGW, P-GW, S-GW

Privilege
Administrator

Syntax

```plaintext
file { format acr { custom1...custom10 } | name { extension string | prefix string } | rotation { record-count num | time-interval sec | volume mb mbytes } }

default file { format acr | name prefix | rotation { record-count | time-interval | volume } }

no file { extension | rotation { record-count | time-interval } }
```

**default**

Returns the command to the default settings for the specified keywords.

**no**

Removes the configuration for the specified parameters.

**format acr { custom1...custom10 }**

Default: `custom1`

Specifies the file format used when storing records on the HD storage device. `custom1` is a vendor-specific file format.

**name { extension string | prefix string }**

Specifies a string to be prepended or appended to the filenames. By default, the policy name is used for the prefix.

- `extension string`: Specifies a file extension to append to the filename. `string` must be an alpha and/or numeric string from 1 to 10 characters.
- `prefix string`: Specifies a file prefix to append to the filename. `string` must be an alpha and/or numeric string from 1 to 63 characters. This parameter replaces the policy name used by default.

**rotation { record-count num | time-interval sec | volume mb mbytes }**

Specifies the triggers that prompt file rotation on the HD storage drive. All options can be configured and upon reaching any of the thresholds, file rotation is initiated.

- `record-count num`: Specifies that file rotation is to occur when the number of records reaches the number configured in this keyword. `num` must be an integer value from 1000 to 65000. Default = 10000
- `time-interval sec`: Specifies that file rotation is to occur a time intervals configured in this keyword. `sec` must be an integer value from 30 to 86400. Default = 3600 (1 hour)
- `volume mb mbytes`: Specifies that file rotation is to occur when the record volume exceeds the value configured in the keyword. `mbytes` must be an integer value from 2 to 40. Default = 4 (mb)
Usage
Use this command to configure file parameters for Diameter records being stored on the HD storage device.

Example
The following command set the file rotation thresholds for files being stored on the HD storage device:

```
file rotation volume mb 4
file rotation record-count 15000
file rotation time-interval 7200
```

The following command replaces the policy name as the prefix of all files being stored through this policy with the prefix `sgw`:

```
file name prefix sgw
```
Chapter 120
HLR Configuration Mode Commands

The HLR Configuration Mode provides the commands and parameters to configure the home location register (HLR) node that is the database containing the subscriber profile and connection information for a specific GPRS/UMTS core network.

The HLR Configuration Mode is a sub-mode derived from the MAP Configuration Mode which controls the MAP service configuration. It is the MAP service that provides the application-layer protocol support used to connect the HLR to other nodes in the network such as the SGSN.
**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the context configuration mode.


**imsi**

This command sets up IMSI (International Mobile Subscriber Identity) -based configuration. (IMSI) prefix which includes the Mobile Country Code (MCC), the Mobile Network Code (MNC).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
```

- **no**
  Removes the imsi-prefix definition from the configuration.

- **any**
  Configures acceptance of any IMSI prefix.

- **starts-with prefix_number**
  Selects IMSI prefix-based routing.
  `prefix_number` is a string of up to 15 integers.

- **imsi**
  Enables configurable default behavior for routing.
  Entering **imsi** with the **any** keyword preserves the default behavior and the E.212 address is used as a destination address and the MAP request will be sent towards the HLR.
  If this keyword is not used with the **any** keyword, then the MAP request will be rejected.

- **isdn isdn_number**
  Defines the E.164 number of the HLR.
  `isdn_number` is a string of integers, up to 15.

- **mobile-global-title mgt_number**
  `mgt_number` is a string of integers, up to 15.

- **point-code pt-code source-ssn ssn**
  Defines the point code for the HLR.
  `pt-code` is a string of digits, up to 11; SS7 format preferred.

- **sgsn-source-address-format point-code-ssn**
  Selects HLR call process according to SCCP calling party address of the SGSN. This will be filled at MAP level, including the ITU point code address.
source-ssn \textit{ssn}

Defines the SSN of the source that will be used for the call filtering.
\textit{ssn}: Must be an integer from 1 to 255.

\textbf{Usage}

Routing will be done according to IMSI parameters configured with this command.

\textbf{Example}

\texttt{imsi starts-with 3 isdn 123456789 sgsn-source-address-form at point-code-ssn}
policy routing

This command configures the policy for the routing of MAP messages. If this command is not configured or disabled (with the `default` keyword), then routing is done according to the configuration of the IMSI parameters.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] policy routing { hlr-isdn | ms-isdn }
```

- **default**
  Resets the policy routing to the system default, disabled.

- **no**
  Removes the policy routing configuration from the system.

- **hlr-isdn**
  Selects HLR-ISDN based routing.

- **ms-isdn**
  Selects mobile station (MS)-ISDN based routing.

**Usage**

Use this command to set the policy for routing MAP messages.

**Example**

```
policy routing hlr-isdn
```
Chapter 121
HNB-GW Service Configuration Mode Commands

The 3G UMTS Home-NodeB Gateway Service Configuration Mode is used to create, provide, and manage the Femto UMTS HNB access with UMTS core network in a 3G UMTS network.
associate gtpu-service

This command associates a previously configured GTP-U service to bind the HNB-GW service with an HNB towards the HNB side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

associate gtpu-service svc_name

no associate gtpu-service

no

Removes the associated GTP-U service from this HNB-GW service configuration.

svc_name

Identifies the name of the GTP-U service preconfigured in Context configuration mode to associate with an HNB-GW service towards the Home-NodeB side. The svc_name must be an alphanumerical string from 1 through 63 characters.

Usage
Use this command to configure GTP-U data plan between HNB-GW service and Home-NodeB. The service defined for GTP-U can be configured in Context configuration mode.

Important: Another GTP-U service can be used to bind the HNB-GW service towards the Core Nework and can be configured in HNB-PS Configuration mode. For more information on GTP-U service configuration, refer GTP-U Service Configuration Mode Commands.

Example
Following command associates GTP-U service named gtpu-hnb1 with specific HNB-GW service towards Home-NodeB side.

     associate gtpu-service gtpu-hnb1
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
radio-network-plmn

This command creates/remove and enters the HNB-RN-PLMN Configuration mode and associate/disassociate it with HNB-GW service. This mode provides configuration mode to configure various parameters for radio network public mobile land networks (PLMNs). A maximum of 16 radio PLMN id can be configured in an HNB-GW service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
radio-network-plmn mcc mcc_value mnc mnc_value [-noconfirm]
no radio-network-plmn mcc mcc_value mnc mnc_value
```

**no**

Removes the configured radio network PLMN identifier for an HNB-GW service.

⚠️ **Caution:** Removing the PLMN identifier is a disruptive operation; the HNB-GW service shall be re-started.

<table>
<thead>
<tr>
<th>mcc mcc_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the mobile country code (MCC) part of radio network PLMN identifier.</td>
</tr>
<tr>
<td><em>mcc_value</em> must be an integer value from 101 through 998.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mnc mnc_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the mobile network code (MNC) part of radio network PLMN identifier.</td>
</tr>
<tr>
<td><em>mcc_value</em> must be an integer value from 01 through 99 or 100 through 998.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-noconfirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates that the command is to execute without any additional prompt and confirmation from the user.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure the radio network PLMN identifier for an HNB-GW service. This command also creates a configuration mode to configure various parameters for defined radio network PLMN identifier in HNB-GW service.

⚠️ **Caution:** Changing or removing the PLMN identifier is a disruptive operation; the MME service shall be re-started.

Entering this command results in the following prompt:

`[context_name]hostname(config-radio-network-plmn)#`

A maximum of 16 radio network PLMN identifiers are supported for an HNB-GW service.
Example

The following command configures the radio network PLMN identifier with MCC value as 102 and MNC value as 20 for an HNB-GW service:

```
radio-network-plmn mmc 102 mnc 20
```
ranap reset

This command configures various RAN Application Part reset procedure parameters with HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
ranap reset { ack-timeout timer_value | guard-timeout g_timer | hnbgw-initiated |
max-retransmissions retries}
```

```
no ranap reset hnbgw-initiated
```

```
default ranap reset { ack-timeout | guard-timeout | hnbgw-initiated | max-
retransmissions}
```

no

Disables the HNB-GW initiated RANAP reset procedure for an HNB-GW service.

---

ack-timeout timer_value

Set the timer value in seconds to wait for Reset Acknowledge from SGSN/MSC. This will be used when HNBGW Initiated Reset procedure is enabled.

`timer_value` must be an integer value from 5 through 10.

Default: 10

---

guard-timeout g_timer_value

Sets the timer value to send Reset Acknowledge to SGSN/MSC. After this duration the HNBGW sends RESET-ACK to SGSN/MSC. This will be used when SGSN/MSC Initiated Reset procedure is enabled.

`g_timer_value` must be an integer value from 5 through 10.

Default: 10

---

hnbgw-initiated

Enables the HNB-GW Initiated RANAP Reset procedures.

Default: Disabled

---

max-retransmission retries

Sets the maximum number of retries allowed for transmission of RESET-ACK message to SGSN/MSC. This parameter is used when HNB-GW initiated Reset procedure is enabled.

`retries` must be an integer value from 0 through 2. When 0 is used retransmission will be disabled.

Default: 1

---

Usage

Use this command to configure the RANAP Reset procedures related parameters in HNB-GW service.
Example
The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-GW service:

```
ranap reset hnbgw-initiated
```
rtp address

This command configures the Real Time Protocol (RTP) address on HNB-GW and send it HNB to map RTP streams with this IP while HNB-GW connects to MSC/VLR through IuCSoIP (IuCS-over-IP) tunnel. This command is used for RTP stream management on HNB-GW.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
rtp address address
no rtp address
```

**no**
Removes the RTP IP address association to be used for communication between HNB and HNB-GW while communicating with MSC/VLR-GW through IuCS over IP tunnel.

**address address**
Specifies the IP address of HNB-GW to use as an end point by HNB and HNB maps the RTP streams with this IP address and HNB-GW communicates with MSC/VLR through IuCS-over-IP Tunnel. 

*address* is the same IP address as assigned to HNB-GW to communicate with HNB and must be an IP address in IPv4 or IPv6 notation.

**Important:** This command cannot be entered more than once. Only one RTP IP address can be configured for one HNB-GW service.

**Usage**

Use this command to enable the HNB-GW IP address as RTP IP address and send the same to HNB to map RTP streams while HNB-GW communicates with MSC/VLR through IuCS-over-IP tunnel. This command is used for RTP stream management on HNB-GW.

**Example**
The following command sets the RTP IP address 1.2.3.4 on HNB-GW to communicate with HNB while using IuCS-over-IP tunnel with CS network:

```
rtp address 1.2.3.4
```
rtp port

This command configures the Real Time Protocol (RTP) port range to listen from HNB while connecting to MSC/VLR through IuCSoIP (IuCS-over-IP) interface support via an HNB-GW service. This command is used for RTP stream management on HNB-GW.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
port range port_start to port_end
default rtp port range
```

```
default
```

Sets the RTP port range to default range from 16384 to 65535.

```
port range range_start to range_end
```

Specifies the port number range to be used by HNB to map the RTP streams and HNB-GW listen on these ports while communicating with MSC/VLR through IuCS-over-IP tunnel.

- `range_start` must be an integer between 16384 through 65535 and should be less than `range_end`.
- `range_end` must be an integer between 16384 through 65535 and should be more than `range_start`.

Default: port 16384 through 65535

**Important:** This command cannot be entered more than once. Only one range of RTP port can be configured for one HNB-GW service.

Usage

**Caution:** This command is NOT active now.

Use this command to assign the RTP port range to be used by HNB to map RTP streams and HNB-GW listen these ports for RTP streams while communicating with MSC/VLR through IuCS-over-IP tunnel. This command is used for RTP stream management on HNB-GW.

Example

The following command sets the RTP port number 20000 to 21000 on HNB-GW to listen from HNB for RTP streams while connecting with MSC/VLR using IuCS-over-IP tunnel.

```
rtp port range 20000 to 21000
```
rtp mux

This command configures the HNB-GW service to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This configuration support is provided for RTP stream management feature on HNB-GW.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

[no | default] rtp mux

no

Removes the configured option to multiplex multiple RTP stream in one packet by Home-NodeB in HNB-GW configuration.

default

Sets the multiplexing option to default state of “disabled”.

Usage

Use this command to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This configuration support is provided for RTP stream management feature on HNB-GW and it is disabled by default.

Example

The following command sets the HNB-GW to allow HNB to multiplex multiple RTP stream in one packet:

rtp mux
This command configures the SCTP IP address and port that will be used for binding the SCTP socket to communicate with the Home-NodeB over Iuh interface with an HNB-GW service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
sctp bind {address address | port port_num }
no sctp bind { address | port }
```

**default**

Sets the SCTP port to default value of 600 to communicate with the Home-NodeB using Iuh interface.

```plaintext
address address
```

Specifies the IP address of HNB-GW in IPv4 or IPv6 notation for the interface configured as Iuh interface to connect with Home-NodeB.

*address* must be an IP address in IPv4 or IPv6 notation.

```plaintext
port port_num
```

Specifies the SCTP port number to communicate with the Home-NodeBs using Iuh interface.

*port_num* must be an integer between 1 through 65535.

**Usage**

Use this command to assign the SCTP IP address and port with SCTP socket on HNB-GW to communicate with the Home-NodeB using Iuh interface. This SCTP configuration provides the IP-address and listen port where HNB-GW service shall bind to listen for incoming SCTP associations from HNB.

**Example**

The following command sets the SCTP port number 999 on HNB-GW to listen from Home-NodeB over Iuh interface:

```plaintext
sctp bind port 999
```

The following command sets the SCTP address 1.2.3.4 of HNB-GW to use with Home-NodeB over Iuh interface:

```plaintext
sctp bind address 1.2.3.4
```
security-gateway aaa

This command associates a preconfigured AAA Servicer group to use authentication parameters for Security Gateway (SeGW) functionality in HNB-GW service. Associated AAA server group is a preconfigured AAA server group configured in Context configuration mode.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```plaintext
security-gateway aaa authentication {first-phase | second-phase} context
ctx_name aaa-group aaa_grp

no security-gateway aaa {attribute calling-station-id | authentication {first-
phase | second-phase}
```

**no**
Removes previously configured AAA authentication or attribute setting from HNB-GW service while using SeGW functionality.

**attribute calling-station-id**  *ms_id*
Specifies the calling station id from where the user placed the call.

**authentication {first-phase | second-phase} context**  *ctx_name aaa-group aaa_grp*
Specifies the AAA authentication parameters to be used while using SeGW functionality in an HNB-GW service.
**first-phase** specifies the parameters to be used for first phase of authentication while using SeGW functionality in an HNB-GW service. This associates the AAA parameters through AAA server group association with in it.
**second-phase** specifies the parameters to be used for second phase of authentication while using SeGW functionality in an HNB-GW service. This associates the AAA parameters through AAA server group association with in it.
**context**  *ctx_name aaa-group aaa_grp* specifies the name of the pre-configured AAA server group and its context to associate AAA parameters to be used for first/second or both phase of authentication while using SeGW functionality in an HNB-GW service.
**ctx_name** specifies the name of the context in which AAA server group is configured.
**aaa_grp** specifies the name of the AAA server group configured in Context configuration mode with AAA parameters which need to be used for first/second or both phase of authentication while using SeGW functionality in an HNB-GW service.

**Important:** For more information on AAA server groups, refer *AAA Server Group Configuration Mode Commands*.
Usage

Use this command to associate or tie the AAA authentication or attribute parameters with an HNB-GW service which is to be used for first/second or both phase of authentication while using SeGW functionality in an HNB-GW service or removing AAA attribute “calling-sation-id” from AAA message. This functionality is part of SeGW configuration support in an HNB-GW service.

⚠️ Caution: This is a critical configuration and need to be configured carefully if Security Gateway (SeGW) functionality is to enable on HNB-GW service.

Example

The following command associates an AAA server group named `sec_gw_grp1` with HNB-GW service to use specific AAA authentication parameters in first phase of authentication and another AAA server group named `sec_gw_grp2` to use different AAA authentication parameter in second phase of authentication. Both AAA server groups are configured in same context named `SeGW_ctx1`:

```
security-gateway aaa authentication first-phase context SeGW1 aaa-group sec_gw_grp1
security-gateway aaa authentication second-phase context SeGW1 aaa-group sec_gw_grp2
```

The following command disables a previously configured AAA authentication parameter for first phase of authentication:

```
no security-gateway aaa authentication first-phase
```
security-gateway bind

This command binds the SeGW in HNB-GW service to a logical IP interface serving as an Iuh interface and associates an IPsec IKV2 crypto-map template to the HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
security-gateway bind address address crypto-template cryp_name

no security-gateway bind address
```

no
Removes a previously configured IPSec IP address use for binding the IKv2 IPSec tunnel (local bind address) to communicate with the Home-NodeBs using Iuh interface.

bind address address
Specifies the IP address in IPv4 or IPv6 notation for the interface configured as an Iuh for IPsec tunnel. This is the IP address where the HNB-GW service is bound and shall be provided to Home-NodeB during HNB-GW discovery.

address specifies the IPsec IP address in IPv4/IPv6 notation to be used for binding the IKEv2 IPSec tunnel (local bind address) to communicate with the Home-NodeBs using Iuh interface.

crypto-template cryp_name
Specifies the Crypto-map template to be used for IPsec IKEv2 tunneling for the interface configured as an Iuh.

cryp_name specifies the name of the pre-configured Crypto-map template which is configured in Crypto-Map Template Configuration Mode and associated with HNB-GW service to create IPSec tunnel with Home-NodeB during HNB-GW discovery procedure on Iuh interface.

Usage
Use this command to associate or tie the HNB-GW service to a specific logical IP address that will be used for binding the Iuh socket to communicate with the Home-NodeB using IPSec tunnel. A maximum of one IP address can be configured with this command for one HNB-GW service.
The HNB-GW passes the IP address during setting up the HNB-GW discovery procedure with the Home-NodeB.

⚠️ Caution: This is a critical configuration. The HNB-GW service can not be started without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration will stop the HNB-GW service.

Example

---

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01
The following command binds the logical IP interface with the address of 1.2.3.4 to the HNB-GW service using existing IPsec Crypto-Map template *crypto1* to establish IPSec tunnel with Home-NodeB:

```
security-gateway bind address 1.2.3.4 crypto-template crypto1
```

The following command disables a binding that was previously configured:

```
security-gateway bind address
```
security-gateway username

This command configures the options related to user name received from MS.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no | default] security-gateway username mac-address-stripping
```

**no**
Disables previously configured option for user name received from MS.

**default**
Sets the user name option configuration of default setting of “Disable”.

**mac-address-stripping**
Default: Disabled
This keyword sets the system to strip the MAC address from the user name received from the MS.

**Usage**
Use this command to set the user name related options. By enabling this option system strips the MAC address from the user name received from MS.

**Example**
The following command sets the system to strip the MAC address from user name received from user MS:

```
security-gateway username mac-address-stripping
```
Chapter 122
HNB-CS Network Configuration Mode Commands

The HNB-CS Network Configuration Mode is used to create, provide, and manage the Circuit Switched (CS) network instance on HNB-GW service to provide HNB access with CS core network in a 3G UMTS network.
associate alcap-service

This command associates a previously defined Access Link Control Application Part (ALCAP) service with the CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs). This configuration is provided to support IuCS-over-ATM functionality.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
associate alcap-service svc_name context ctx_name
no associate alcap-service
```

- `svc_name`:
  Identifies the name of the ALCAP service preconfigured in Context configuration mode to associate with an HNB-CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs). The `svc_name` must be a preconfigured ALCAP service. Only one instance of this command can be configured.

**Caution:** If this CLI is not configured any RAB-ASST-REQ message requesting AAL2 connection setup shall be rejected with an appropriate cause.

- `context ctx_name`:
  Specifies the name of the context in which ALCAP service is configured. The `ctx_name` must be an existing context name in which this ALCAP service is configured.

**Usage**

Use this command to configure IuCS-over-ATM support. This association of ALCAP protocol service configuration in HNB-CS network instance provides multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).

**Caution:** If this CLI is not configured any RAB-ASST-REQ message requesting AAL2 connection setup shall be rejected with an appropriate cause.

**Important:** This command must not be used more than once to configure IuCS-over-ATM support.

**Example**

Cisco ASR 5000 Series Command Line Interface Reference
Following command associates ALCAP service `alcap_svc1` configured in context named `Ctx_alcap1` with specific HNB-CS network instance:

```
associate alcap-service alcap_svc1context Ctx_alcap1
```
associate rtp pool

This command associates a previously defined RTP pool (IP pool) with the CS network instance to be used for assignment of IP address/port as RTP streams end point address over IuCS interface. This configuration support is provided for RTP stream management feature in an HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
associate rtp pool pool_name context ctx_name
no associate rtp pool
```

**No**

Removes the associated RTP pool (IP pool) from this HNB-CS network instance configuration.

```
pool_name
```

Identifies the name of the RTP IP pool preconfigured in Context configuration mode to associate with an HNB-CS network instance to be used for assignment of IP address/port over the IuCS interface RTP streams. The `pool_name` must be an existing IP pool name configured in Context configuration mode.

**Important:** For IP pool (RTP pool) configuration, refer Context Configuration Commands Mode chapter.

```
context ctx_name
```

Specifies the name of the context in which RTP pool (IP pool) is configured. The `ctx_name` must be an existing context name in which this IP pool is configured.

Usage

Use this command to associate RTP pool (IP Pool) with an HNB-CS network instance for allotment of IP address/port over IuCS interface for RTP streams across all sessions. A fixed range of RTP ports from 5000 through 65000 shall be used to allocate to RTP stream.

**Important:** This command must be used to provide IP address/port for RTP streams end point address over IuCS interface.

**Important:** This configuration support is provided for RTP stream management feature on an HNB-GW service.

Example

Following command associates RTP pool named `rtp_1` with specific HNB-CS network instance:
associate rtp pool rtp_1
**associate sccp-network**

This command associates a predefined Signaling Connection Control Part (SCCP) network id with the CS network instance in order to route the messages towards MSC/VLR over IuCS interface.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

associate-sccp-network sccp_net_id

no associate-sccp-network

**Usage**

Use this command to associate a preconfigured SCCP network id over IuCS interface in HNB-GW service to connect with CS network elements; i.e. MSC.

⚠️ **Caution:** The SCCP network id must be defined in Global Configuration mode before using it with this command.

🔥 **Important:** A single SCCP network configuration instance can not be shared with multiple HNB-CS network instances.

**Example**

Following command associates SCCP network 2 with specific HNB-CS network instance:

```
associate-sccp-network 2
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Change the mode back to the Exec mode.
**exit**

Exits the current mode and returns to the previous mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Return to the previous mode.
**HNB-CS Network Configuration Mode Commands**

**msc point-code**

This command is used to configure default MSC point-code with HNB-CS network instance. This command is used when HNB-GW is to be connected to only one MSC with in a CS network or as default MSC for all HNBs connected through specific HNB-CS network instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[no] msc point-code point_code
```

**no**

Removes the configured default MSC point code from specific HNB-CS network instance.

⚠️ **Caution:** Removing the MSC point code is a disruptive operation and affects all HNB sessions which are connected to particular MSC through an HNB-CS network instance.

**Usage**

Use this command to configure a default MSC to which HNB will connect for CS network access through HNB-GW service.

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

⚠️ **Important:** This command can be entered only once. If entered again the previous value shall be overwritten.

**Example**

The following command configures a default MSC with point code **01.201.101** for HNBs to access CS network through HNB-GW service in this HNB-CS network instance:
msc point-code 101.201.101
Chapter 123
HNB-PS Network Configuration Mode Commands

The HNB-PS Network Configuration Mode is used to create, provide, and manage the Packet Switched (PS) network instance on HNB-GW service to provide HNB access with PS core network in a 3G UMTS network.
associate gtpu-service

This command associates a previously configured GTP-U service to bind the HNB-GW service to provide a GTP-U tunnel with an SGSN towards the core network side. A GTP-U service must be configured in Context configuration mode before using this configuration.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax
associate gtpu-service svc_name context ctx_name

no associate gtpu-service

no

Removes the associated GTP-U service from this HNB-GW service configuration.

svc_name

Identifies the name of the GTP-U service preconfigured in Context configuration mode to associate with an HNB-GW service towards the Home-NodeB side. The svc_name is name of a preconfigured GTP-U service.

context ctx_name

Specifies the name of the context in which GTP-U service is configured. The ctx_name must be an existing context name in which this GTP-U service is configured.

Usage
Use this command to configure GTP-U data plan tunnel between HNB-GW service and GSNs in core network. The service defined for GTP-U tunnel must be configured in Context configuration mode.

Important: Another GTP-U service can be used to bind the HNB-GW service to GTP-U tunnel with HNB in HNB access network and can be configured in HNB-GW Service Configuration mode. For more information on GTP-U service configuration, refer GTP-U Service Configuration Mode Commands.

Example
Following command associates GTP-U service gtpu_svc1 configured in context named Ctx_gtpu1 with specific HNB-PS network instance for GTP-U tunnel towards GSN in core network:

associate gtpu-service gtpu_svc1 context Ctx_gtpu1
associate-sccp-network

This command associates a previously defined Signaling Connection Control Part (SCCP) network id with the PS network instance in order to route the messages towards SGSN over IuPS interface.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
associate-sccp-network sccp_net_id
no associate-sccp-network
```

**Usage**

Use this command to associate a predefined SCCP network id with the IuPS interface in HNB-GW service to connect with PS network elements; i.e. SGSN.

**Caution:** The SCCP network id must be defined in Global Configuration mode before using it with this command.

**Important:** A single SCCP network id can not be shared with multiple HNB-PS network instances.

**Example**

Following command associates SCCP network id 2 with specific HNB-PS network instance:

```
associate-sccp-network 2
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Return to the previous mode.
sgsn point-code

This command is used to configure default SGSN point-code with HNB-PS network instance. This command is used when HNB-GW is to be connected to only one SGSN with in a PS network or as default SGSN for all HNBs connected through specific HNB-PS network instance.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

[no] sgsn point-code point_code

no

Removes the configured default SGSN point code from specific HNB-PS network instance.

⚠️ Caution: Removing the SGSN point code is a disruptive operation and affects all HNB sessions which are connected to particular SGSN through an HNB-PS network instance.

point_code

Specifies SS7 address of default SGSN in PS network in point code value to this configured HNB-PS network instance.

point_code must be in SS7 point code dotted-decimal ###.###.### format or 8-digit decimal ####### format.

Only one instance of this command can be configured.

Usage

Use this command to configure a default SGSN to which HNB will connect for PS network access through HNB-GW service.

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.

- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

⚠️ Important: This command can be entered only once. If entered again the previous value shall be overwritten.

Example

The following command configures a default SGSN with point code 101.201.101 for HNBs to access PS network through HNB-GW service in this HNB-PS network instance:
sgsn point-code 101.201.101
This HNB Radio Network PLMN configuration mode provides configuration to define the radio network PLMN parameters related to the HNB-GW connection with UMTS Femto radio network.
associate cs-network

This command associates a preconfigured circuit switched (CS) network within an HNB radio network PLMN with HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
[no] associate cs-network cs_name [lac lac]
```

**no**
Disassociates/removes the configured CS network with an HNB radio network PLMN configured in HNB-GW service mode.

**cs_name**
Specifies the name of a preconfigured CS network in Global configuration mode with `cs-network` command and to be associated with an HNB radio network PLMN configured in HNB-GW service mode. To configure CS network, refer *HNB-CS Configuration Mode Commands* chapter.

**lac lac_id**
This keyword defines the granularity level of circuit switch network to a location area code (LAC) level to be associated with radio network PLMN in HNB-GW service. `lac_id` must be an integer between 1 and 65535.

**Usage**

Use this command to associate pre-defined CS networks with a radio network PLMN in an HNB-GW service.

The circuit switched network comprises of one or more MSCs, where CS-domain IU-connections shall be routed. In a typical deployment HNB-GW is connected to only one MSC. However due to Iu-flex and networks-sharing requirements, HNB-GW can be connected to more than one MSCs as well.

Another scenario when HNB-GW can be connected to multiple MSCs is when a set of HNBs should be connected to a particular MSC based on their UTRAN location or geographical location.

This command provides configuration to have one or more MSCs such that these are used in load-shared (IuFlex) or network-shared mode. If location based distribution of HNBs to MSCs is desired then more than one circuit switched network configuration will be required.

This configuration allows association of a circuit switched network with a radio network PLMN and granularity can either be at the PLMN level or at the level of a location area (LAC) in that PLMN.

To configure CS network, refer *HNB-CS Configuration Mode Commands* chapter.

**Example**
The following command associates a CS network `umts1` with radio network PLMN with a granularity of LAC 234:
associate cs-network umts1 lac 234
associate ps-network

This command associates a preconfigured packet switched (PS) network within an HNB radio network PLMN with HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

[no] associate ps-network ps_name [lac lac [rac rac]]

no

Disassociates/removes the configured PS network with an HNB radio network PLMN configured in HNB-GW service mode.

ps_name

Specifies the name of a preconfigured PS network in Global configuration mode with ps-network command and to be associated with an HNB radio network PLMN configured in HNB-GW service mode. To configure PS network, refer HNB PS Configuration Mode Commands chapter.

lac lac_id

This keyword defines the granularity level of packet switched network to a location area code (LAC) level to be associated with radio network PLMN in HNB-GW service. lac_id must be an integer between 1 and 65535.

rac rac_id

This keyword defines the granularity level of packet switched network to a radio area code (RAC) level to be associated with radio network PLMN in HNB-GW service. rac_id must be an integer between 1 and 65535.

Usage

Use this command to associate pre-defined PS networks with HNB radio network PLMN in an HNB-GW service.

The packet switched network comprises of one or more SGSNs where PS-domain IU-connections shall be routed. In a typical deployment HNB-GW is connected to only one SGSN. However with IuFlex and network-sharing functionality, HNB-GW can be connected to more than one SGSNs as well. Another scenario when HNB-GW can be connected to multiple SGSNs is when a set of HNBs should be connected to a particular SGSN based on their UTRAN location or geographical location. This command provides configuration to have one or more to have one or more SGSNs such that these are used in load-shared (iu-flex) or network-shared mode. If location based distribution of HNBs to SGSNs is desired then more than one packet switched network configuration will be required.

This command allows association of a packet switched network with a radio network PLMN and granularity could either be at the PLMN level or at the level of a location area code (LAC) in that PLMN or at the level of a routing area code (RAC) in that LAC.

To configure PS network, refer HNB-PS Configuration Mode Commands chapter.
Example
The following command associates a PS network `umts_psi` with radio network PLMN with a granularity of LAC 234 and RAC as 123:

```
associate ps-network umts_psi lac 234 rac 123
```
end

Exits the configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the Global configuration mode.
rnc-id

This command configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-GW service to provide RNC identifier to HNB during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
[rno] rnc-id rnc_id [lac lac_id [rac rac_id | cell-id cell_id]]
```

- **no**
  Deletes the LAC and RAC information from the system configuration.

- **rnc-id**
  Specified the RNC id to be configured in radio network PLMN associated with HNB-GW and to be provided to HNB during HNB-REGISTRATION procedure from HNB-GW. It also configures RNC Id for all HNBs operating in a particular PLMN.
  
  - `rnc_id` must be an integer between 1 and 65535.

- **lac lac_id**
  This keyword defines the granularity level of location of HNB to a location area code (LAC) level and configures RNC ID for all HNBs operating in particular location-area.
  
  - `lac_id` must be an integer between 1 and 65535.

- **rac rac_id**
  This keyword defines the granularity level of location of HNB to a routing area code (RAC) level and configures RNC ID for all HNBs operating in particular routing area.
  
  - `rac_id` must be an integer between 1 and 65535.

- **cell-id cell_id**
  This keyword defines the granularity level of location of HNB to a UTRAN cell level and configures RNC ID for all HNBs operating in particular UTRAN cell area.
  
  - `cell_id` must be an integer between 1 and 65535.

Usage

Use this command to configure RNC id for Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

When HNB-REGISTRATION request is received the RNC Id is looked up by matching the parameters received in the request. The most specific entry that matches the request shall have the highest priority. For example in the following configuration:
rnc-id 257 lac 1 cell-id 3
rnc-id 258 lac 1 rac 2
rnc-id 259 lac 1
rnc-id 260

• If request is received with LAC=1, RAC=2, and Cell-Id=3, the selected RNC id will be 257.
• If request is received with LAC=1, RAC=3, and Cell-Id != 3, the selected RNC id will be 258.
• If request is received with LAC=1 and any other values of RAC and Cell-id, the selected RNC id will be 259. For all other requests 260 will be returned.

Example
Following command will configure the HNB-GW service to return RNC id as 102 when HNB-REGISTRATION request is received with LAC 1, and RAC 2:

```
rnc-id 102 lac 1 rac 2
```

Following command will configure the HNB-GW service to return RNC id as 102 when HNB-REGISTRATION request is received with LAC 1 and cell-id 4:

```
rnc-id 102 lac 1 cell-id 5
```
Chapter 125
HSGW Service Configuration Mode Commands

The HSGW Service Configuration Mode is used to create and manage a configuration allowing the HSGW to communicate, send and receive call data, and session flows to/from a eAN/PCF in an eHRPD network.

**Important:** This appendix will be added to the CLI Reference when the product releases. Use this appendix in conjunction with the latest release of the Command Line Interface Reference.
associate

Associates accounting policies and QCI-QoS mapping parameters with this HSGW service.

Product
HSGW

Privilege
Administrator

Syntax

```
associate { accounting-policy name | qci-qos-mapping name }
```

```
o associate { accounting-policy [ name ] | qci-qos-mapping }
```

```
no
```

Removes the specified associated policy or mapping from the service.

```
accounting-policy name
```

Specifies the accounting policy to associate with the HSGW service. `name` must be an existing accounting policy and be from 1 to 63 alpha and/or numeric characters.

```
qci-qos-mapping name
```

Associates the HSGW service with QCI to QoS mapping parameters. `name` must be an existing QCI-QoS mapping configuration and be from 1 to 63 alpha and/or numeric characters.

QCI-QoS mapping is configured through the `qci-qos-mapping` command in the Global Configuration Mode.

Usage
Use this command to associate an accounting policy with the HSGW service.

Example
The following command associates an accounting policy named `acct2` to the HSGW service:

```
associate accounting-policy acct2
```
bind address

Binds the service to a logical IP interface serving as the A10 interface and specifies the maximum number of subscribers that can access this service over the configured interface.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
bind address ip_address [ max-subscribers num ]
no bind address
```

- **no**
  Removes the interface binding from this service.

- **ip_address**
  Specifies the IPv4 address of the interface configured as the A10/A11 interface. *ip_address* is specified in dotted decimal notation.

- **max-subscribers num**
  Default: 250000
  Specifies the maximum number of subscribers that can access this service on this interface. *num* must be configured to an integer between 0 and 2,500,000.

**Important:** The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

**Usage**

Associate the HSGW service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an A10/A11 interface that provides the session connectivity to/from an eAN/PCF. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of A10/A11 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to
Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example
The following command would bind the logical IP interface with the address of 112.334.556.778 to the HSGW service and specifies that a maximum of 200,000 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 112.334.556.778 max-subscribers 200000
```
**context-retention-timer**

Configures the maximum number of consecutive seconds that a UE session context (which includes the LCP, authentication and A10 session context for a given UE) is maintained by the HSGW before it is torn down.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
context-retention-timer timeout [ sec ]
[ default | no ] context-retention-timer timeout
```

- **default**
  Disables the timer.

- **no**
  Disables the timer.

- **timeout [ sec ]**
  Default: 60
  Specifies the amount of time, in seconds, that the session context is maintained before it is disassembled. `sec` must be an integer value from 1 to 3600.

**Usage**

Use this command to configure a timer to retain session contexts for a specified amount of time before disassembling it.

**Example**

The following command allows the HSGW to maintain session contexts for 120 seconds before tearing them down:

```
context-retention-timer timeout 120
```
**data-available-indicator**

Enable sending Data Available Indicator extension in A10/A11 Registration Reply messages.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
data-available-indicator
```

**Usage**

Use this command to enable the sending of the Data Available Indicator extension in A10/A11 Registration Reply messages.
data-over-signaling

Enable the data-over-signaling marking feature for A10 packets.

Product
HSGW

Privilege
Administrator

Syntax

[ default | no ] data-over-signaling

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables the data-over signaling feature for A10 packets.</td>
</tr>
</tbody>
</table>

| no |
| Disable the data-over signaling feature for A10 packets. |

Usage

Use this command to enable or disable the data-over signaling feature for A10 packets.
**dns-pgw**

Identifies to the HSGW service the location of the DNS client. The DNS client is used to identify a FQDN for the peer P-GW. This command defaults to the same context as the HSGW service.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**
```
dns-pgw context name
```

- **default**
  Returns the command to its default setting of the current context.

- **no**
  Removes the configured DNS client context name from this service.

- **context name**
  Specifies the context in which the DNS client is configured. `name` must be an existing context and be from 1 to 63 alpha and/or numeric characters.

**Usage**
Use this command to identify to the HSGW service the context where the DNS client is configured.

**Example**
The following command identifies the context where the DNS client is configured as `isp3`:
```
dns-pgw context isp3
```
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the previous mode.
fqdn

Configures the Fully Qualified Domain Name (FQDN) for this HSGW.

**Product**

HSGW

**Privilege**

Administrator

**Syntax**

fqdn domain_name

[ default | no ] fqdn

default

Returns the command to the default setting of “null”.

no

domain_name

Specifies an FQDN for the HSGW. domain_name must be from 1 to 256 alpha and/or numeric characters.

**Usage**

Use this command to configure an FQDN for this HSGW. The FQDN is used by a P-GW (APN FQDN) when selecting an HSGW.

**Example**

The following command configures this HSGW with an FQDN of abc123.com

```
  fqdn abc123.com
```
fragment

Enables/Disables PPP payload fragmentation.

Product
HSGW

Privilege
Administrator

Syntax

[ default | no ] fragment ppp-data

---

default
Returns the command to its default setting of enabled.

---

no
Disables PPP payload fragmentation.

Usage

Use this command to enable or disable PPP payload fragmentation.
**gre**

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the HSGW service.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
gre { checksum | checksum-verify | flow control [ action { disconnect-session | resume-session } ] [ timeout msecs ] + | ip-header-dscp value { all-control-packets | setup-packets-only } | reorder-timeout msecs | segmentation | sequence-mode { none | reorder } | sequence-numbers | threegpp2-ext-headers qos-marking }

default gre { checksum | checksum-verify | flow-control | ip-header-dscp | reorder-timeout | sequence-mode | sequence-numbers | threegpp2-ext-headers qos-marking }

no gre { checksum | checksum-verify | flow-control | ip-header-dscp | segmentation | sequence-numbers | threegpp2-ext-headers qos-marking }
```

**default**
Restores the specified parameter to its default setting.

**no**
Disables the specified functionality.

**checksum**
Default: disabled
Enables the introduction of the checksum field in outgoing GRE packets.

**checksum-verify**
Default: disabled
Enables verification of the GRE checksum (if present) in incoming GRE packets.

**flow-control [ action { disconnect-session | resume-session } ] [ timeout msecs ] +**
Default: no GRE flow-control
Enables 3GPP2 GRE flow control which causes the HSGW to send flow control enabled Normal Vendor Specific Extensions (NVSE) in A11 RRPs.

**action { disconnect-session | resume-session }**:
Default: disconnect-session
Specifies the action to be taken when timeout is reached:

- **disconnect-session**: Ends the session and releases the call.
- **resume-session**: Switches flow control to XON and resumes delivery of packets to the RAN.
**timeout**`msecs`
Default: 1000 milliseconds (10 seconds)
Sets the amount of time wait for an XON indicator from the RAN (after receiving an XOFF). Also sets the action to be taken if the timeout limit is reached.

`msecs`: Specifies the amount of time in milliseconds before the timeout is reached. `msecs` must be an integer from 1 through 1000000.

---

**ip-header-dscp** `value { all-control-packets | setup-packets-only }`
Default: Disabled
Used to configure the QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- `value`: Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F.
- `all-control-packets`: Dictates that the DSCP marking is to be provided in all GRE control packets.
- `setup-packets-only`: Dictates that the DSCP marking is to be provided only in GRE setup packets.

---

**reorder-timeout**`msecs`
Default: 100
Configures max number of milliseconds to wait before processing reordered out-of-sequence GRE packets.
`msecs` must be an integer from 0 through 5000.

---

**segmentation**
Default: disabled
Enables GRE Segmentation for the HSGW service.

---

**sequence-mode { none | reorder}**
Default: none
Configures handling of incoming out-of-sequence GRE packets.

- `none`: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.
- `reorder`: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:
  - The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
  - The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
  - An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
  - A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.
**sequence-numbers**

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenceed.

**threegppp2-ext-headers qos-marking**

When threegppp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the HSGW will include the QoS optional data attribute in the GRE 3gpp2 extension header. The **no** keyword, enables qos-marking in the GRE header based on the tos value in the header.

**Usage**

Use the **no gre sequence-numbers** command to disable the inclusion of GRE sequence numbers in the A10 data path. More Usage....

**Example**

The following command configures the HSGW service to support the inclusion of GRE sequence numbers in outgoing traffic:

```
gre sequence-numbers
```
Sets the use of Robust Header Compression (RoHC) and enters the HSGW Service ROHC Configuration Mode where RoHC parameters are configured for the service.

Configures the local User Datagram Protocol (UDP) port for the A10/A11 interface IP socket.

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```plaintext
ip { header-compression rohc | local-port number | source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num } }

default ip { local-port | source-violation drop-limit | period | reneg-limit }

no { header-compression rohc | ip source-violation clear-on-valid-packet }
```

---

**default**
Resets the keyword to its default value.

**no**

- **header-compression rohc**: Removes the RoHC configuration from this service.
- **ip source-violation clear-on-valid-packet**: Disables the ability of the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

---

**header-compression rohc**
Specifies that Robust Header Compression will be applied to sessions using this service and enters the HSGW Service RoHC Configuration Mode where RoHC parameters are configured.

**local-port number**
Default: 699
Specifies the UDP port number.
`number` can be any integer value between 1 and 65535.

**source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num }**

**clear-on-valid-packet**
Default: disabled
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.
**drop-limit num**  
Default: 10  
Sets the number of allowed source violations within a detection period before forcing a call disconnect. If num is not specified, the value is set to the default.  
num can be any integer value from 1 to 1000000.

**period secs**  
Default: 120  
The length of time, in seconds, for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.  
The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If secs is not specified, the value is set to the default.  
secs must be an integer value from 1 to 1000000.

**reneg-limit num**  
Default: 5  
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If num is not specified, the value is set to the default.  
num can be any integer value from 1 to 1000000.

**Usage**

**Header Compression RoHC**: Use this command to specify that sessions using this service will have Robust Header Compression applied and configure parameters supporting RoHC.  
Entering this command results in the following prompt:  
```shell
[context_name]hostname(config-ip-header-compression-rohc)#
```
HSGW Service RoHC Configuration Mode commands are defined in the HSGW Service RoHC Configuration Mode Commands chapter.

**Local Port**: Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the HSGW.

**Important**: The UDP port setting on the PCF must match the local-port setting for the HSGW service on the system in order for the two devices to communicate.

**Source Violation**: This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two HSGWs a number of times during a handoff scenario.  
This function operates in the following manner:  
When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period.  
Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.  
For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.  
If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.  
If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by 1. If the reneg-limit counter equals zero, the drop-limit is decremented by half.
Example
The following command specifies a UDP port of 3950 for the HSGW service to use to communicate with the PCF on the A10/A11 interface:

```
ip local-port 3950
```

The following command sets the drop limit to 15 and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```
**lifetime**

Specifies the time that an A10 connection can exist before its registration is considered expired.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
lifetime time

[ default | no ] lifetime
```

- **default**
  Resets the lifetime value to the default setting of 1800 seconds.

- **no**
  Specifies that an A10 connection can exist for an infinite amount of time.

- **time**
  Default: 1800
  Specifies the time that an A10 connection can exist before its registration is considered expired.
  `time` is measured in seconds and can be configured to any integer value between 1 and 65534.

**Usage**

Use this command to set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, the connection is terminated automatically.

**Example**

The following command specifies a time of 3600 seconds (1 hour) for subscriber sessions on this HSGW service:

```
lifetime 3600
```
max-retransmissions

Configures the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

Product
HSGW

Privilege
Administrator

Syntax

max-retransmissions count

default max-retransmissions

default
Rests the maximum number of allowed retransmissions to the default value of 5.

count
Default: 5
Specifies the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

count can be configured to any integer value between 1 and 1000000.

Usage
Use this command to limit the number of retransmissions to an eAN/PCF before marking it as unreachable. If the value configured is reached, the call is dropped.

Example
The following command configures the maximum number of retransmissions for the HSGW service to 3:

max-retransmissions 3
mobile-access-gateway

Identifies the mobile access gateway (MAG) context through which MIPv6 calls are to be routed.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
mobile-access-gateway context context_name [ mag-service service_name ]
```

```
o mobile-access-gateway context
```

```
no
```

Removes the configured MAG context route from this service.

```
context context_name [ mag-service service_name ]
```

Specifies the name of the context and, optionally, the service through which MIPv6 sessions are to be routed. `context_name` must be an existing context and be from 1 to 79 alpha and/or numeric characters. `service_name` must be an existing Mag service and be from 1 to 63 alpha and/or numeric characters.

**Usage**

Use this command to specify where MIPv6 sessions are routed through this service.

**Example**
The following command identifies the MAG context `MAG1` as the context through which MIPv6 sessions are to be routed and further narrows the route by specifying the service name (`mag_serv3`):

```
mobile-access-gateway context MAG1 mag-service mag_serv3
```
plmn id

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming, or belongs to this network.

Product
HSGW

Privilege
Administrator

Syntax

```
plmn id mcc number mnc number
```

- `mcc number`: Specifies the mobile country code (MCC) portion of the PLMN’s identifier. `number` is the PLMN MCC identifier and must be an integer value between 100 and 999.
- `mnc number`: Specifies the mobile network code (MNC) portion of the PLMN’s identifier. `number` is the PLMN MNC identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.

Usage
The PLMN identifier is used to aid the HSGW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service. The configured IDs are used in Diameter-EAP-Request messages (as a Visited-Network-Identifier AVP).

Example
The following command configures the PLMN identifier with an MCC of 462 and MNC of 2:

```
plmn id mcc 462 mnc 02
```
policy overload

Specifies how an HSGW service should handle overload conditions.

Product
HSGW

Privilege
Administrator

Syntax

\[ \text{policy overload \{ redirect address [ weight weight\_num ] [ address2 [ weight weight\_num ] \ldots address16 [ weight weight\_num ] \] | reject [ use reject-code { admin-prohibite | insufficient-resources } ] \}} \]

\[ \text{default policy overload} \]

\[ \text{no policy overload \{ redirect address [ address2 ] \ldots [ address16 ] } \]

---

**default**

Returns the command to its default setting of “reject” with the “admin-prohibited” code.

---

**no**

Removes a specified “redirect address” from this service.

---

**redirect address [ weight weight\_num ] [ address2 [ weight weight\_num ] \ldots address16 [ weight weight\_num ] ]**

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HSGW service rejects new sessions with an A11 Registration Reply Code of 88H (unknown HSGW address) and provides the IP address of an alternate HSGW. This command can be issued multiple times.

*address*: The IP address of an alternate HSGW expressed in IPv4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

*weight weight\_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified, the entry is automatically assigned a weight of 1 (default). *weight\_num* must be an integer value from 1 through 10.

---

**reject [ use reject-code { admin-prohibite | insufficient-resources } ]**

This option will cause any overload traffic to be rejected. The HSGW sends an A11 Registration Reply Code of 82H (insufficient resources).

*use-reject-code admin-prohibited*: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code “insufficient resources”. This is the default behavior.

*use-reject-code insufficient-resources*: When this keyword is specified and traffic is rejected, the error code “insufficient resources” is returned instead of the error code admin prohibited.
Usage
Policies can be implemented to dictate HSGW service behavior for overload conditions. The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system. The system automatically invokes the overload policy when an on-line software upgrade is started. Use the `no policy overload` command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the `default policy` command.

The chassis is shipped from the factory with the policy options overload disabled.

Example
The following command configures the HSGW service to redirect overload traffic to two IPv4 address, one priority weighted 1 and the other priority weighted 5:

```
policy overload redirect 1.2.3.4 weight 1 1.2.3.5 weight 5
```
**profile-id-qci-mapping**

Associates a configured mapping table for RP QoS Profile ID to LTE QoS Class Index (QCI) mapping with this service.

**Product**

HSGW

**Privilege**

Administrator

**Syntax**

```
profile-id-qci-mapping name
no profile-id-qci-mapping [ name ]
```

**no**

Removes all profile maps or a specific profile map from this service.

**name**

Specifies the name of the table to be associated with this service. *name* must be an existing Profile ID - QCI Mapping table and be from 1 to 63 alpha and/or numeric characters in length.

**Usage**

Use this command to associate the HSGW service with a configured Profile ID - QCI Mapping table. The table is configured in the Global Configuration Mode using the `profile-id-qci-mapping-table` command.

**Example**

The following command associates a Profile ID - QCI Mapping table named *table3* with this service:

```
profile-id-qci-mapping table3
```
**registration-deny**

Configures parameters related to registration rejection.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
registration-deny { handoff connection-setup-record-absent | newcall connection-setup-record-absent } [ use-deny-code { poorly-formed-request | reason-unspecified } ]
```

**handoff connection-setup-record-absent**

When enabled, the HSGW denies or discards handoff sessions that do not have an Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default HSGW behavior is to accept such requests.

**newcall connection-setup-record-absent**

When enabled, the HSGW denies or discards new sessions that do not have the airlink connection setup record in the RRQ.

```
[ use-deny-code { poorly-formed-request | reason-unspecified } ]
```

Sets the specified Registration Deny Code when denying a new call or handoff because of a missing connection setup record.

**Usage**

Use this command to configure parameters relating to the rejection of registration requests.

**Example**

The following command denies registration for registration requests missing the connection setup record and replies with a use deny code of “poorly formed request”:

```
registration-deny handoff connection-setup-record-absent use-deny-code poorly-formed-request
```
retransmission-timeout

Configures the maximum allowable time for the HSGW service to wait for a response from the eAN/PCF before it attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF) or marks the eAN/PCF as unreachable.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
retransmission-timeout time
{ default | no } retransmission-timeout
```

- **default**
  Resets the timeout setting to the default value of 3.

- **no**
  Deletes a previously configured timeout value.

- **time**
  Default: 3
  Specifies the maximum allowable time, in seconds, for the HSGW service to wait for a response from the eAN/PCF before it: a) attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF) or b) marks the eAN/PCF as unreachable.
  `time` must be an integer value between 1 and 1000000.

**Usage**

Use the retransmission timeout command in conjunction with the `max-retransmissions` command in order to configure the HSGW services behavior when it does not receive a response from a particular PCF.

**Example**

The following command configures a retransmission timeout value of 5 seconds:

```
retransmission-timeout 5
```
**setup-timeout**

The maximum amount of time allowed for session setup.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
setup-timeout seconds
[ default| no ] setup-timeout
```

- **default**
  Rests the command to the default value of enabled with a timeout of 60 seconds.

- **no**
  Disables the feature.

- **seconds**
  Default: 60
  The maximum amount of time, in seconds, to allow for setup of a session in this service. *seconds* must be an integer value from 1 through 100000.

**Usage**

Use this command to set the maximum amount of time allowed for setting up a session.

**Example**

The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

```
setup-timeout 300
```
**spi remote-address**

Configures the security parameter index (SPI) between the HSGW service and the eAN/ePCF. This command also configures the redirection of call based on the PCF zone.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
spi remote-address {pcf_ip_address | ip_addr_maskCombo} spi-number number {
encrypted secret enc_secret | secret secret } [ description string ] [ hash-algorithm { md5 | rfc2002-md5 } ] [ replay-protection { nonce | timestamp } ] [ timestamp-tolerance tolerance ] [ zone zone_id ]
```

```
no spi remote-address pcf_ip_address spi-number number
```

- **pcf_ip_address**: Specifies the IP address of the ePCF. pcf_ip_address is an IP address expressed in IPv4 dotted decimal notation or IPv6 colon separated notation.
- **ip_addr_maskCombo**: Specifies the IP address of the PCF and specifies the IP address network mask bits. ip_addr_maskCombo must be specified using the form ‘IP Address/Mask Bits’ where the IP address must either be an IPv4 address expressed in dotted decimal notation or an IPv6 address expressed in colon separated notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

**spi-number number**

Specifies the SPI (number) which indicates a security context between the PCF and the HSGW. number can be configured to any integer value between 256 and 4294967295.

**encrypted secret enc_secret | secret secret**

Configures the shared-secret between the HSGW service and the PCF. The secret can be either encrypted or non-encrypted.

- **encrypted secret enc_secret**: Specifies the encrypted shared key (enc_secret) between the PCF and the HSGW service. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.
- **secret secret**: Specifies the shared key (secret) between the PCF and the HSGW services. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

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

**description string**

This is a description for the SPI. string must be an alpha and/or numeric string from 1 through 31 characters.
### hash-algorithm \{ md5 | rfc2002-md5 \}

Default: md5
Specifies the hash-algorithm used between the HSGW service and the PCF.
- **md5**: Configures the hash-algorithm to implement MD5.
- **rfc2002-md5**: Configures the hash-algorithm to implement keyed-MD5.

### replay-protection \{ nonce | timestamp \}

Default: timestamp
Specifies the replay-protection scheme that should be implemented by the HSGW service.
- **nonce**: Configures replay protection to be implemented using NONCE.
- **timestamp**: Configures replay protection to be implemented using timestamps.

### timestamp-tolerance tolerance

Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.
- **tolerance** is measured in seconds and can be configured to any integer value between 0 and 65535.

### zone zone_id

Specifies the different PCF zones to configure in HSGW service. Mapping of a zone-number to a set of HSGWs can be done per HSGW service basis.
- **zone_id** must be an integer value between 1 and 32. A maximum of 32 PCF zones can be configured for a HSGW service.

### Usage

An SPI is a security mechanism configured and shared by the PCF and the HSGW service. Please refer to IOS 4.1 and RFC 2002 for additional information.
Multiple SPIs can be configured if the HSGW service is communicating with multiple eAN/PCFs.

### Important:

The SPI configuration on the PCF must match the SPI configuration for the HSGW service on the system in order for the two devices to communicate properly.

This command used with the **zone** keyword redirects all calls on the basis of PCF zone to the specific HSGW on the basis of parameters configured using the **policy pcf-zone-match** command.

### Example

The following command configures the HSGW service to use an SPI of 256 when communicating with a PCF with the IP address **192.168.0.2**. The key that would be shared between the PCF and the HSGW service is **q397F65**.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command creates the configured SPI of **400** for an PCF with an IP address of **172.100.3.200** and zone id as **11**:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```
HSGW Service Configuration Mode Commands

spi remote-address
**unauthorized-flows**

Configures the service to wait a specified number of seconds before triggering a QoS update to downgrade an unauthorized flow.

**Product**
HSGW

**Privilege**
Administrator

**Syntax**

```
unauthorized-flows qos-update wait-timeout seconds
[ default | no ] unauthorized-flows qos-update wait-timeout
```

- **default**
  Returns the command to its default setting of

- **no**
  Removes the configure wait-timeout setting for this service.

- **qos-update wait-timeout seconds**
  Specifies the number of seconds to wait before triggering the QoS update to downgrade the unauthorized flow. `seconds` must be an integer value from 1 to 65534.

**Usage**

Use this command to specific a wait timeout trigger for flows that are unauthorized by policy rules received via the Gxa interface from the PCRF. When the wit timer expires, the HSGW triggers a QoS update to downgrade the unauthorized flow.

**Example**

The following command configures the HSGW service to apply the wait time of 30 seconds after receiving an flow unauthorized by the PCRF:

```
unauthorized-flow qos-update wait-timeout 30
```
Chapter 126
HSGW Service RoHC Configuration Mode Commands

The HSGW Service RoHC Configuration Mode is used to configure RoHC parameters for the service.

```
Exec Mode
  configure
    context name
      hsgw-service name
        HSGW Service Configuration Mode
          ip header-compression rohc
            HSGW Service RoHC Config Mode
```
cid-mode

This mode allows you to configure options that apply during RoHC compression for the service.

Product
HSGW

Privilege
Administrator

Syntax

cid-mode \{ large | small \} max-cid integer

default cid-mode

default
Reset all options in the RoHC Profile Compression Configuration mode to their default values.

large
Use large packets with optional information for RoHC

small
This is the default packet size.
Use small RoHC packets.

max-cid integer
Default: 15
The highest context ID number to be used by the compressor. integer must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.

Usage
Use this command to set the RoHC packet size and define the maximum

Example
The following command sets large RoHC packet size and sets the maximum CID to 100:
cid-mode large max-cid 100

The following command sets the cid-mode to the default settings of small packets and max-cid 0:
default cid-mode
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
mrru

This command sets the size of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments. The size includes the CRC. If MRRU is negotiated to be 0, no segment headers are allowed on the channel.

Product

HSGW

Privilege

Administrator

Syntax

```plaintext
mrru num_octets

default mrru
```

- `default`
  reset the value of this command to its default setting

- `num_octets`
  Default: 0
  This is the number of octets for the maximum size of the largest reconstructed reception unit allowed. `num_octets` must be an integer from 0 through 65535.

Usage

Use this command to set the size, in octets, of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments.

Example

The following command sets the largest reconstructed reception unit to 1024 octets:

```
mrru 1024
```

The following command resets the mrru size to its default of 0 octets:

```
default mrru
```
profile

This command specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

Product
HSGW

Privilege
Administrator

Syntax

```
profile { [ esp-ip ] [ rtp-udp ] [ udp-ip ] [ uncompressed-ip ] }
```

default profile

default
Default: esp-ip rtp-udp udp-ip uncompressed-ip
Returns the RoHC profile configuration to its default setting.

esp-ip
This enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.

rtp-udp
This enables RoHC Profile 0x0001 which is for RTP/UDP/IP compression

udp-ip
This enables RoHC Profile 0x0002 which is for UDP/IP compression, compression of the first 12 octets of the UDP payload is not attempted.

uncompressed-ip
This enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.

Usage
Us this command to specify the RoHC header compression profiles to use.

Example
The following command sets the profiles to use as esp-ip and rtp-udp:

```
profile esp-ip rtp-udp
```
Chapter 127
IKEv2 Security Association Configuration Mode
Commands

The IKEv2 Security Association Configuration Mode is used to configure a Security Association at the outset of an IPsec session. A security association is the collection of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. In normal bi-directional traffic, the flows are secured by a pair of security associations.

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

Sets the default properties for the selected parameter.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default { encryption | group | hmac | lifetime | prf }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption</td>
<td>Default algorithm for the IKEv2 IKE SA is AES-CBC-128</td>
</tr>
<tr>
<td>group</td>
<td>Default Diffie-Hellman group is Group 2</td>
</tr>
<tr>
<td>hmac</td>
<td>Default IKEv2 IKE SA hashing algorithm is SHA1-96</td>
</tr>
<tr>
<td>lifetime</td>
<td>Default lifetime for SAs derived from this transform-set is 86400 seconds.</td>
</tr>
<tr>
<td>prf</td>
<td>Default PRF for the IKEv2 IKE SA is SHA1.</td>
</tr>
</tbody>
</table>

**Usage**
Configure default parameters for the IKEv2 IKE SA transform-set.

**Example**
Use the following configuration to set the default encryption algorithm:

```
default encryption
```
encryption

Configure the appropriate encryption algorithm and encryption key length for the IKEv2 IKE security association. AES-CBC-128 is the default.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc }
default encryption
```

<table>
<thead>
<tr>
<th>3des-cbc</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Triple DES.” Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cypher keys.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>aes-cbc-128</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits. This is the default setting for this command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>aes-cbc-256</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>des-cbc</th>
</tr>
</thead>
</table>

Usage
IKEv2 requires a confidentiality algorithm to be applied in order to work. In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly-generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity. Because RFC 4307 calls for interoperability between IPsec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPsec in order for there to be an acceptable match during the IKE message exchange. Because of RFC4307, in IKEv2, there is no viable NULL option, it is available for testing only.

Example
The following command configures the encryption to be the default aes-cbc-128:

```
default encryption
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Returns to the previous mode.
group

Configure the appropriate key exchange cryptographic strength by applying a Diffie-Hellman group. Default is Group 2.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

group { 1 | 2 | 5 | 14 }
default group

1
Configures crypto strength at the Group 1 level. Lowest security.

2
Configures crypto strength at the Group 2 (default) level. Medium security.
This is the default setting for this command.

5
Configures crypto strength at the Group 5 level. Higher security.

14
Configures crypto strength at the Group 14 level. Highest security

Usage
Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process in IKEv2. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.
Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group 14 provides 2048 bits of encryption strength.
Configuring a DH group also enables Perfect Forward Secrecy, which is disabled by default.

Example
This command configures security at the default level (Group 2):

default group
**hmac**

Configures the IKEv2 IKE SA integrity algorithm. Default is SHA1-96.

**Product**  
PDIFF

**Privilege**  
Security Administrator, Administrator

**Syntax**

```  
hmac { md5-96 | sha1-96 }  
default hmac
```

**md5-96**  
HMAC-MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

**sha1-96**  
HMAC-SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. This is the default setting for this command.

**Usage**  
IKEv2 requires an integrity algorithm be configured in order to work. A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated to 96 bits and transmitted. The authenticator value is reconstituted by the receiver and the first 96 bits are compared for a 100 percent match. Because RFC 4306 calls for interoperability between IPsec and IKEv2, the IKEv2 integrity algorithms must be the same as those configured for IPsec in order for there to be an acceptable match during the IKE message exchange.

**Example**  
The following command configures the default HMAC value (SHA1-96):

```  
default hmac
```
lifetime

Configure the lifetime of a security association (SA) in seconds. Default timeout time is 86400 seconds.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
lifetime sec
```

default lifetime

```
lifetime sec
Default: 86400
Sets the value of the timeout parameter. sec must be an integer from 60 - 86400.
```

Usage

The secret keys that are used for various aspects of a configuration should only be used for a limited amount of time before timing out. This exposes a limited amount of data to the possibility of hacking. If the SA expires, the options are then to either close the SA and open a new one, or renew the existing SA.

Example

The following command sets the lifetime timeout to be the default value (86400):

```
default lifetime
```
prf

Select one of the HMAC integrity algorithms to act as the IKE Pseudo-Random Function. A PRF produces a string of bits that an attacker cannot distinguish from random bit string without knowledge of the secret key. The default is SHA1.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
prf { md5 | sha1 }

default prf
```

---

| md5 |
| MD5 uses a 128-bit secret key and produces a 128-bit authenticator value. |

| sha1 |
| SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. SHA-1 is considered cryptographically stronger than MD5, but it takes more CPU cycles to compute. This is the default setting for this command. |

---

Usage
The prf is used for generating keying material for all the cryptographic algorithms used in both the IKE-SA and the CHILD_SAs.

Example
This configuration sets the prf to be the default value (sha1):

```
default prf
```
Chapter 128
IMS Authorization Service  Configuration Mode
Commands

IP Multimedia Sub-system (IMS) authorization service is used to configure authorization parameters to manage policy control functions and Gx and Ty interface support with Diameter based procedures for flow based charging within a context. The system uses Gx/Gy andTx/Ty functionality based on the charging policy and rules configured to flow based charging for a subscriber session.

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

Exits the IMS Authorization Configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to change to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
p-cscf discovery

This command defines the method of Proxy-Call Session Control Function (P-CSCF) discovery to be used.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
p-cscf discovery {table { 1 | 2 } [ algorithm { ip-address-modulus | msisdn-modulus | round-robin } ] | diameter-configured } [ default | no ] p-cscf discovery
```

- **default**
  Sets the P-CSCF discovery to default parameter.

- **no**
  Removes/deletes configured parameters for P-CSCF discovery.

- **table { 1 | 2 }**
  This keyword specifies that which P-CSCF table is to be used to obtain the primary and secondary P-CSCF addresses. Total 2 tables can be configured for P-CSCF discovery.

- **algorithm { ip-address-modulus | msisdn-modulus | round-robin }**
  Default: round-robin.
  This keyword specifies the algorithm to select the row from the P-CSCF table to be used for P-CSCF discovery.
  - **ip-address-modulus**: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
  - **msisdn-modulus**: This algorithm divides the MSISDN value in binary without the leading “+” of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
  - **round-robin**: This algorithm rotates all rows in the active table for selection of the row in round-robin way. If no algorithm is specified this is the default behavior.

- **diameter-configured**
  This option enables the table number and algorithm specified by the `diameter host-select table` configuration in Policy Control Configuration mode.
  If the primary host in that configuration is down it assumes that the primary P-CSCF in the row of P-CSCF table is also down, and it does not return that IP address in the create PDP context response.
  This option also performs the deactivation processing of the PDP contexts when Diameter Policy Control Application (DPCA) switches, host tables as detailed in the `diameter host-select` command description in Policy Control Configuration mode.
Usage
Use this command to configure the table and row selection methods to select IP address/host address for P-CSCF discovery.

Example
The following command specifies table 1 with round-robin algorithm to select the rows with IP address for P-CSCF discovery.

```
p-cscf discovery table 1 algorithm round-robin
```
p-cscf table

This command adds/appends rows with primary and/or secondary IPv4/IPv6 address to a P-CSCF discovery table with precedence for Proxy-Call Session Control Function (P-CSCF) discovery.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
p-cscf table { 1 | 2 } row-precedence precedence_value { address ip_address | ipv6-address ipv6_address } [ secondary { address ip_address | ipv6-address ipv6_address } ]
```

```
no p-cscf table { 1 | 2 } row-precedence precedence_value
```

**no**
Removes/deletes configured row with precedence in specified table for P-CSCF discovery address.

```
{ 1 | 2 }
```
Specifies which P-CSCF table is to be used to add/append the primary and secondary P-CSCF addresses. Two tables can be configured for P-CSCF discovery address.

**row-precedence precedence_value**
This keyword adds/appends the row with the specified row-precedence to the P-CSCF address table. In StarOS 8.1 and later, `precedence_value` must be an integer from 1 through 128, and a maximum of 128 rows can be added to a table. In StarOS 8.0, `precedence_value` must be an integer from 1 through 100, and a maximum of 16 rows can be added to a table.

**secondary**
Specifies the secondary IPv4/IPv6 address to be entered in P-CSCF table rows.

**address ip_address**
Specifies the primary and/or secondary IPv4 address for P-CSCF discovery table. This keyword, if used with `secondary` keyword, specifies the secondary IPv4 address. `ip_address` must be an IPv4 IP address entered using dotted decimal notation.

**ipv6-address ipv6_address**
Specifies the primary and/or secondary IPv6 address for P-CSCF discovery table. This keyword, if used with `secondary` keyword, specifies the secondary IPv6 address. `ipv6_address` must be an IPv6 IP address entered using colon (:) separated notation.

**Usage**
Use this command to add rows with primary and/or secondary IP addresses for P-CSCF discovery. The row is added with the specified row-precedence. The operator can add/remove rows to the table that is not currently selected by the `diameter host-select table` command in Policy Control Configuration Mode.

**Example**
The following command adds a row in `table 2` with primary IP address `1.2.3.4`, secondary IP address as `5.6.7.8`, and row-precedence value as `20` for P-CSCF discovery.

```plaintext
p-cscf table 2 row-precedence 20 address 1.2.3.4 secondary 5.6.7.8
```
policy-control

This command enters the Policy Control Configuration mode for Diameter Policy Control Application (DPCA) to configure Diameter authorization and policy control parameter for IMS authorization.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] policy-control
```

**no**

Disables the pre-configured policy control parameters for IMS authorization in this IMS authorization service.

**Usage**

Use this command to enter the Policy Control Configuration Mode to configure the policy control parameters for Diameter authorization and charging policy in IMS Authorization Service.

**Example**

```plaintext
policy-control
```
qos-update-timeout

This command sets the Quality of Service update timeout for a subscriber in IMS authorization service.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
qos-update-timeout timeout_duration
[ no ] qos-update-timeout
```

**no**
Disables the pre-configured QoS update timeout parameter in this IMS authorization service.

```
timeout_duration
```
Default: 60
Specifies the duration of timeout in seconds, and must be an integer from 0 through 3600.

**Usage**
Use this command to set the maximum time to wait for a subscriber to initiate the update QoS procedure in IMS authorization service.

**Example**
Following command sets the QoS update timeout to 90 seconds.

```
qos-update-timeout 90
```
reauth-trigger

This command specifies the trigger events to initiate re-authorization for a subscriber in IMS authorization service.

**Important:** This command now moved to Policy Control Config mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default ] reauth-trigger{ all | { an-gw-change | bearer-loss | bearer-recovery |
plmn-change | policy-failure | qos-change | rat-change | sgsn-change | tft-change |
tft-delete } + }
```

**Default**
Sets the pre-configured Re-authorization trigger to default value.

**all**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on all events listed in this command.

**an-gw-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber whose access network gateway changed.

**bearer-loss**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on loss of bearer or service.

**bearer-recovery**
Sets the IMS authorization service to initiate re-authorization process for a subscriber when a bearer or service recovered after loss of bearer or service.

**default-bearer-qos-change**
Sets the IMS authorization service to initiate re-authorization process when QoS is changed and DEFAULT_EPS_BEARER_QOS_CHANGE event triggered for the default EPS bearer context of a subscriber in LTE network.

**plmn-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Public Land Mobile Network (PLMN) of subscriber.
IMS Authorization Service Configuration Mode Commands

**policy-failure**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on failure of credit and charging policy for subscriber.

**qos-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Quality of Service level/rating of subscriber.

**rat-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Radio Access Type (RAT) of subscriber node.

**sgsn-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in SGSN for subscriber node.

**tft-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Traffic Flow Template (TFT) of subscriber session.

**tft-delete**
Sets the IMS authorization service to initiate re-authorization process for a subscriber when Traffic Flow Template (TFT) of subscriber session is deleted by a system administrative user.

**Usage**
Use this command to set the triggers to initiate QoS re-authorization process for a subscriber in IMS authorization service.

**Example**
Following command sets the re-authorization trigger to **bearer-loss**, so that re-authorization of subscriber session is initiated on loss of bearer.

```
reauth-trigger bearer-loss
```
signaling-flag

This command specifies whether a request for a PDP context dedicated to signaling (for IMS sessions) should be granted or denied.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
signaling-flag { deny | permit }
[ default ] signaling-flag
```

**default**
Sets the signaling flag to default mode of deny.

**deny**
Default: Enabled.
When specified this keyword denies the request for a signaling PDP context for IMS session and keeps signaling co-existed with other traffic on PDP contexts.

**permit**
Default: Disabled.
When specified this keyword permit the request for a signaling PDP context for IMS session and a separate signaling context activated.

**Usage**

Use this command to allow or deny the activation of dedicated PDP context for signaling. The user equipment (UE) may indicate that the PDP context should be dedicated for IP multimedia (IM) signaling by setting the IP Multimedia Core Network (IM CN) signaling flag in the Protocol Configuration Options (PCO).

The **deny** option causes the system to inform the UE that the PDP context will not be dedicated for IM signaling and signaling will co-exist with other traffic on PDP context.

The **permit** option is used to activate the signaling context for signal traffic and the other traffic uses other PDP context for traffic with the following destinations:

- Towards the DHCP and DNS servers for the IMS domain.
- Towards the P-CSCF(s).

The UE is not trusted to follow these restrictions, and the system monitors and restricts the traffic from the dedicated PDP context. The **signaling-flow class-map** command is used to configure the restrictions.

**Example**

Following command denies the request for a signaling PDP context for IMS session.
default signaling-flag
signaling-flow permit

This command specifies the packet filters and policy servers for bandwidth control and singling context enforcement that define the traffic that is allowed through the dedicated signaling context.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
signaling-flow permit server-address ip_address [ server-port { port_num | range start_port to end_port } ] [ description STRING ]

[ no ] signaling-flow permit server-address ip_address [ server-port { port_num | range start_port to end_port } ]
```

**no**
Disables the signaling flow option configured with his command.

**server-address ip_address**
The server address `ip_address` refers to the destination IP address in uplink packets, and the source IP address in downlink packets.
`ip_address` is IPv4/IPv6 address in standard notation and can be used with sub-net mask.
A maximum of 16 signaling server address can be configured per IMS Authorization service.

**server-port { port_num | range start_port to end_port }**
Specifies the TCP/UDP port number(s) of the server and to be used for communication.
`port_num` must be an integer from 1 through 65535.
`range start_port to end_port` provides the option to configure the range of ports on server for communication.
`start_port` must be an integer from 1 through 65535 but lesser than `end_num`, and `end_port` must be an integer from 1 through 65535 but greater than `start_num`

**description STRING**
Specifies the customized description for configured signaling server.
`STRING` must be an alpha and/or numeric string with maximum of 64 characters.

Usage
Traffic that matches any instance of the signaling-flow command will be forwarded via the signaling PDP context. In addition, the policy server gives policy gates to use for the signaling PDP context.

Example
Following command sets the packet filter server address to `1.2.3.4` with port number `1234` for packet filtering.
signaling-flow permit

signaling-flow server-address 1.2.3.4 server-port 1234
traffic-policy general-pdp-context

This command specifies the action on packets which do not match any policy gates in the general purpose PDP context.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

```
traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }

default traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink }
```

**default**
Sets the default traffic policy for packets without any policy gate match in general purpose PDP context. By default packets which do not have any matching policy gate are forwarded.

**no-matching-gates**
This keyword applies traffic policy for packets which do not match any policy gate.

**direction { downlink | uplink }**
Specifies the direction of traffic to apply this traffic policy in general PDP context.
- **downlink**: specifies the traffic from system to MN. Default is set to forward.
- **uplink**: specifies the traffic from MN to system. Default is set to forward.

**forward**
Default: Enabled.
This option forward the packets which do not match any policy gates.

**discard**
Default: Disabled.
This option discards the packets which do not match any policy gates.

Usage
This command provides configuration on traffic policy applied on packets which are not matching any policy gate in general PDP context. Packets can either forwarded or discarded on the basis of operators configuration.
This command needs to be configured once for downlink and once for uplink separately.

Example
Following command discard uplink packets which do not match any policy gate in general purpose PDP context.
traffic-policy general-pdp-context no-matching-gates direction uplink discard
Chapter 129
IMS Sh Service Configuration Mode Commands

The IMS Sh Interface Configuration Mode is used to configure various Diameter parameters in order for:
PDIF to communicate with the HSS server. HSS server is used for MAC address validation in the IKEv2 exchanges to set up SAs and for storing part of the user profile.
SCM to communicate with the HSS server. HSS server is used for retrieval and update of call feature parameters and call restriction data.

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

This command configures Diameter parameters.

Product
PDIF, SCM

Privilege
Administrator

Syntax

    diameter { dictionary { custom1 | standard } | endpoint string }

    default diameter { dictionary | endpoint }

    no diameter endpoint

    no
    Removes previously configured endpoint.

    default
    Configures parameters to the default value.

    dictionary
    Specifies the dictionary to use.
    • custom1: A custom dictionary
    • standard: The standard dictionary

    Important: SCM uses only the standard dictionary.

    endpoint string
    Selects an endpoint to use in the configuration.
    string must be the endpoint name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage
The Diameter endpoint contains information on the peer names and IP addresses and port, and the local IP address to use for Diameter.
You can have more than one Diameter endpoint configured on the chassis and the ims-sh-service needs to know which Diameter endpoint to use. This command is to select the appropriate Diameter endpoint, even if only one has been configured.

Example
The following example selects a diameter endpoint diam1:
diameter endpoint diam1
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to change to the Exec Mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
failure-handling

This command configures the action to take in the event of an HSS server request failure.

Product
PDIF, SCM

Privilege
Administrator

Syntax

[ default ] failure-handling { profile-update-request | user-data-request } { { diameter-result-code result_code [ to result_code ] } | timeout } action { continue | retry-and-terminate | terminate } }

default
 Resets configuration for the specified keyword to the default setting.

profile-update-request
 Configures failure-handling as a result of a profile update request error.

user-data-request
 Configures failure-handling as a result of a user data request.

diameter-result-code result_code [ to result_code ]
The Result-Code data field contains a space representing errors. Diameter provides the following classes of errors, all identified by the thousands digit in the decimal notation:
- 3xxx (Protocol Errors)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failure)

result_code specifies either a result code value (diameter-result-code 3001) or a range of result code values (diameter-result-code 3000 to 9999) to which the failure-handling applies.

action
 Configures the action to take depending on the diameter-result-code:
- Continue the session
- Retry and then terminate
- Terminate the session

request-timeout action
 Configures the action to take as a result of a request timeout error:
- Continue the session
- Retry and then terminate
- Terminate the session
**Usage**

Configures all failure-handling parameters.

**Example**

The following command configures profile-update-request failure-handling using a result-code configuration with the terminate session option:

```
failure-handling profile-update-request diameter-result-code 3005 to 3600
action terminate
```
request

Configures application request timeout.

Product
PDIF, SCM

Privilege
Administrator

Syntax

request timeout secs

[ no | default ] request timeout

no
Disables a configured timeout request.

default
Default: 300 seconds
Resets configuration to the default setting.

request timeout secs
Configures the request timeout in seconds.
secs must be an integer from 1 through 300.

Usage
Specifies the session request timeout period in seconds after which the request is deemed to have failed.

Example
The following example configures the default timeout request of 300 seconds:

default request timeout
Chapter 130
IPMS Client Configuration Mode Commands

The IPMS Client Configuration Mode is used to enable the IPMS client service on an Access Gateway and to set basic service wide options in a context.

**Important:** This is a license enabled external application support. For more information on this product, refer to the IPMS Installation and Administration Guide.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          ipms
            IPMS Configuration Mode
```

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
**exit**

Exits the current mode and returns the CLI session to the previous parent mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the parent CLI mode.
export keys

This command enables the encryption key export in specific key exchange events to IPMS server from IPMS-enabled AGW.

Important: This is a license enabled customer specific command.

Product
IPMS

Privilege
Security Administrator, Administrator

Syntax

no
Removes the configured source IP address from this context for IPMS client communication with IPMS server.

ikev2
This keyword enables the security association (SA) key export for Internet Key Exchange (IKEv2) protocol to IPMS server.

Usage
Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

Example
The following command assigns the IP address 1.2.3.4 to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

source address 1.2.3.4
heartbeat

This command configures the IPMS heartbeating between IPMS-enabled AGW and IPMS server.

**Product**
IPMS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
heartbeat [ period dur [ permitted-failure no_of_failures ] ]
[ no | default ] heartbeat
```

- **default**
  Configures the heartbeat period and permitted number of failure to default value of 10 seconds and 1 failure respectively.

- **no**
  Disables/removes the configured heartbeat period and permitted number of failure.

- **period dur**
  Default: 10
  Specifies the periodicity in seconds of heartbeat messages.
  `dur` is the duration in second between two heartbeat messages and must be an integer value from 1 through 3600.

- **permitted-failure no_of_failures**
  Default: 1
  Specifies the number of errors/failures allowed before declaring an IPMS server as dead/unreachable.
  `no_of_failures` is the number of errors/failure of heartbeat message response and must be an integer value from 1 through 10.

**Usage**

Use this command to configure the heartbeat message periodicity and permissible failure of heartbeat message response before declaring an IPMS server as dead or unreachable. When an IPMS server is declared down an SNMP trap is sent.

**Example**

Following command configures the heartbeat message periodicity to 5 second and number of failures allowed as 3 to determine an IPMS server as dead.

```
heartbeat period 5 permitted-failure 3
```
server

This command configures the IPMS server address and ports on which IPMS client on IPMS-enabled AGW communicates. This is the IP address and port range of IPMS server.

**Product**
- IPMS

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
server address <ip_address> [ start-port <start_port> [ end-port <end_port> ]] [ secondary ]
```

[ no ] server address <ip_address>

- **no**
  - Removes the configured IPMS server IP address and port range from this context.

- **address <ip_address>**
  - Specifies the IP address of the IPMS server to which the IPMS client service communicates. This is the address which is used by IPMS client service to locate the IPMS server.
  - A maximum of 4 IPMS servers can be configured with this command in one context.
  - `ip_address` must be an IP v4 address in dotted decimal notation.

- **[ start-port <start_port> [ end-port <end_port> ]]**
  - Default: 45001 source port
  - 45005 end port
  - Specifies the range of UDP ports on which IPMS client communicates with IPMS server.
  - start-port `start_port` is the starting port number and must be an integer value in the range from 1 through 65535 but less than `end_port`, if `end_port` is specified.
  - end-port `end_port` is the end port number and must be an integer value in the range from 1 through 65535 but more than `start_port`.

- **secondary**
  - The secondary keyword is used to configure the specified server address as secondary IP address on the IPMS client interface.

**Usage**

Use this command to configure/remove the IPMS servers. Up to 4 different IPMS servers can be configured with this command. UDP port number can also be configured with this command. IPMS client will search for this IP address to push the event and traffic logs.

**Example**
The following command configures IPMS server having IP address 1.2.3.4 in the IPMS client service export the event and traffic logs for intelligent packet monitoring functionality. It also specifies the UDP port range from 48000 to 48005 for communication.

```
server address 1.2.3.4 start-port 48000 end-port 48005
```
source

This command configures the source address of IPMS client in this context to communicate with IPMS server. This is the IP address for IPMS client on the chassis.

**Product**
IPMS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] source address ip_address
```

- **no**
  Removes the configured source IP address IPMS client from this context for communication with IPMS server.

- **address ip_address**
  Specifies the IP address of the IPMS client on the AGW in this context. This is the address which is bound to the IPMS client service in this context.
  *ip_address* must be an IP v4 address in dotted decimal notation.

**Usage**
Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

**Example**
The following command assigns the IP address 1.2.3.4 to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

```
source address 1.2.3.4
```
Chapter 131
IPSec Transform Set Configuration Mode Commands

The IPSec Transform Set Configuration Mode is used to configure IPsec security parameters. There are two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). AH may be considered redundant as ESP can provide the same authentication services that AH does.

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

Set or restore the default mode for a given parameter

Product  
PDIF

Privilege  
Security Administrator, Administrator

Syntax

default { encryption | group | hmac | mode }

default { encryption | group | hmac | mode }

Set the defaults for the IPSec transform-set as follows:

- **encryption**: Default Child SA IPSec ESP algorithm is AES-CBC-128
- **group**: Default Diffie-Hellman group algorithm is none. This also deactivates PFS.
- **hmac**: Default Child SA IPSec hashing algorithm is SHA1-96.
- **mode**: Default Child SA IPSec Mode is Tunnel.

Usage

Defines the default values for the Child SA IPSec transform-set.

Example

Use the following configuration to set the default mode to Tunnel:

default mode
encryption

Configures the appropriate IPsec ESP encryption algorithm and encryption key length. AES-CBC-128 is the default.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```plaintext
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc | null }
default encryption
```

3des-cbc

“Triple DES.” Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cipher keys.

aes-cbc-128

Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits. This is the default setting for this command.

aes-cbc-256

Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.

des-cbc


null

The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

Usage
In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity.

Because RFC 4307 calls for interoperability between IPsec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPsec in order for there to be an acceptable match during the IKE message exchange. In IKEv2, there is no NULL option.

Example
The following command configures the encryption to be the default aes-cbc-128:
default encryption
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Returns to the previous mode.
group

Configure the appropriate key exchange cryptographic strength and activate Perfect Forward Secrecy by applying a Diffie-Hellman group.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
group { 1 | 2 | 5 | 14 | none }
default group
```

- **default group**
  Configures the default crypto strength to be `none` and disables Perfect Forward Secrecy.

- **1**
  Configures crypto strength at the Group 1 level. Lowest security.

- **2**
  Configures crypto strength at the Group 2 level. Medium security.

- **5**
  Configures crypto strength at the Group 5 level. Higher security.

- **14**
  Configures crypto strength at the Group 14 level. Highest security.

- **none**
  Applies no group and disables Perfect Forward Secrecy. This is the default.

Usage

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.

Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group 14 2048 bits. Selecting a group automatically activates Perfect Forward Secrecy. The default value is `none`, which disables PFS.

Example

This command configures security at Group 2 and activates PFS:
group 2
**hmac**

Configures the IPsec ESP integrity algorithm.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
hmac { md5-96 | sha1-96 | null }
default hmac
```

**default**

Configures the default hmac value of sha1-96.

**md5-96**

MD5-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

**sha1-96**

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value.

This is the default setting for this command.

**null**

Configures the hmac value to be null. The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

**Usage**

HMAC is an encryption technique used by IPsec to make sure that a message has not been altered. A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated to 96 bits and transmitted. The authenticator value is reconstituted by the receiver and the first 96 bits are compared for a 100 percent match. Because RFC 4306 calls for interoperability between IPsec and IKEv2, the IKEv2 integrity algorithms must be the same as those configured for IPsec in order for there to be an acceptable match during the IKE message exchange.

**Example**

The following command configures the default HMAC value (SHA1-96):

```
default hmac
```
hmac
mode

Configures the security of IP datagrams based on header placement. Tunnel mode applies security to a completely encapsulated IP datagram, while Transport does not. Default is Tunnel mode.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
mode { transport | tunnel }
default mode
```

**transport**

In Transport mode, the IPSec header is applied only over the IP payload, not over the IP header in front of it. The AH and/or ESP headers appear between the original IP header and the IP payload, as follows:
Original IP header, IPSec headers (AH and/or ESP), IP payload (including transport header).
Transport mode is used for host-to-host communications and is generally unsuited to PDIF traffic.

**tunnel**

In Tunnel mode, the original IP header is left intact, so a complete IP datagram is encapsulated, forming a virtual tunnel between IPSec-capable devices. The IP datagram is passed to IPSec, where a new IP header is created ahead of the AH and/or ESP IPSec headers, as follows:
New IP header, IPSec headers (AH and/or ESP), old IP header, IP payload.
Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-network and host-to-host communications over the Internet.
This is the default setting for this command.

**Usage**

IPSec modes are closely related to the function of the two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). Both of these protocols provide protection by adding to a datagram a header (and possibly other fields) containing security information. The choice of mode does not affect the method by which each generates its header, but rather, changes what specific parts of the IP datagram are protected and how the headers are arranged to accomplish this.

**Example**
The following command configures the default Tunnel mode:

```plaintext
default mode
```
Chapter 132
IPSG RADIUS Server Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Server Configuration Mode is used to create and configure IPSG services within the current system context. The IPSG RADIUS Server Mode configures the system to receive RADIUS accounting requests as if it is a RADIUS Accounting Server, and reply after accessing those requests for user information.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          ipsg-service name mode radius-server
            IPSG RADIUS Server Config Mode
```

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

bind

Binds the IPSG RADIUS Server service to a logical AAA interface and specifies the number of allowed subscriber sessions.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

```
bind { accounting-proxy address address | address address } [ max-subscribers num | port num | source-context name ]
bind authentication-proxy address address [ acct-port port | auth-port port | max-subscribers num | source-context name ]
```

```
no bind
```

no

Removes the binding for the service.

```
accounting-proxy address address | address address } [ max-subscribers num | port num | source-context name ]
```

accounting-proxy address address: Specifies IP address of the interface where accounting proxy requests are received by this service. address must be specified using standard IPv4 or IPv6 dotted decimal notation.

address address: Specifies IP address of the interface where accounting requests are received by this service. address must be specified using standard IPv4 or IPv6 dotted decimal notation.

max-subscribers num: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

In Release 8.x, num must be an integer from 0 through 300000.
In Release 9.x and later, num must be an integer from 0 through 4000000.

port num: Default: 1813. Specifies the port number of the interface where accounting requests are received by this service. num must be an integer from 0 through 65535.

source-context name: Specifies the source context where RADIUS accounting requests are received. name must be an alpha and/or numeric string of 1 through 79 characters in length. This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

```
authentication-proxy address address [ acct-port port | auth-port port | max-subscribers num | source-context name ]
```

authentication-proxy address address: Specifies the IP address of the interface where authentication proxy requests are received by this service. address must be specified using standard IPv4 or IPv6 dotted decimal notation.
Important: Enabling authentication proxy also enables accounting proxy.

```
acct-port port: Default: 1813. Specifies the port number of the interface where accounting proxy requests are received by this service. port must be an integer from 0 through 65535.
auth-port port: Default: 1812. Specifies the port number of the interface where authentication proxy requests are received by this service. port must be an integer from 0 through 65535.
max-subscribers num: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit. In Release 8.x, num must be an integer from 0 through 3000000. In Release and 9.0 later, num must be an integer from 0 through 4000000.
source-context name: Specifies the source context where RADIUS accounting requests are received. name must be an alpha and/or numeric string of 1 through 79 characters in length. This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.
```

Usage

Use this command to bind the IPSG RADIUS Server service to a logical AAA interface and specify the number of allowed subscriber sessions. If the AAA interface is not located in this context, configure the source-context parameter.

Use the accounting and authentication proxy settings to enable RADIUS proxy server functionality on the IPSG. These commands are used when the NAS providing the RADIUS request messages is incapable of sending them to two separate devices. The IPSG in RADIUS Server mode proxies the RADIUS request and response messages while performing the user identification task in order to provide services to the session.

Example

The following command binds the service to a AAA interface with and IP address of 1.2.3.4 located in the source context named aaa_ingress:

```
bind address 1.2.3.4 source-context aaa_ingress
```
connection authorization

Sets the RADIUS authorization password that must be matched by the RADIUS accounting requests received by this service.

**Product**  
IPSG

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
connection authorization { [ encrypted ] password password }
```

```
no connection authorization
```

- `encrypted`: Indicates that the received RADIUS authorization password is encrypted.
- `password`: Specifies the password that must be matched by incoming RADIUS accounting requests. `password` must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

The IPSG RADIUS server service does not terminate RADIUS user authentication so the user password is unknown. Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

**Example**

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests sent to this service. The password must be encrypted and the example provided is the word “secret”.

```
connection authorization encrypted password secret
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to change to the Exec Mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
profile

Configures the service to use APN or subscriber profiles.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

profile { APN | subscriber }

default profile

<table>
<thead>
<tr>
<th>APN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the service to support APN configuration required to enable Gx support. This is the default setting for this command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>subscriber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the service to support subscriber profile lookup.</td>
</tr>
</tbody>
</table>

Usage

Use this command to set the service to support APN profiles (supporting Gx through the enabling of `ims-auth-service`) or for basic subscriber profile lookup.
radius accounting

Specifies the IP address and shared secret of the RADIUS accounting client from which RADIUS accounting requests are received. The RADIUS client can be either the access gateway or the RADIUS accounting server depending on which device is sending accounting requests.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

```
radius accounting { { client { ip_address | ip_address/mask } [ encrypted ] key secret [ dictionary dictionary ] [ disconnect-message { dest-port destination_port } ] } } | { interim create-new-call } }

no radius accounting client { ip_address | ip_address/mask }

default radius accounting interim create-new-call
```

- **no**
  Removes the RADIUS accounting client address identifier from the service.

- **ip_address | ip_address/mask**
  Specifies the IP address and, optionally, subnet mask of the RADIUS client from which RADIUS accounting requests are received. `ip_address` and `ip_address/mask` must be specified using standard IPv4 or IPv6 dotted decimal notation. Up to 16 addresses can be configured.

- **dictionary dictionary**
  Specifies what dictionary database to use. The possible values for `db` are described in the following table:

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>custom(x)</td>
<td>These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. (x) is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-835</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-vsa1</td>
<td>This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.</td>
</tr>
<tr>
<td>starent-vsa1-835</td>
<td>This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.</td>
</tr>
</tbody>
</table>

```
[ encrypted ] key secret
```

**encrypted**: Specifies that the shared key between the RADIUS client and this service is encrypted.

**key secret**: Specifies the shared key between the RADIUS client and this service. **secret** must be an alpha and/or numeric string of 1 through 127 characters in length, and is case sensitive.

```
disconnect-message [ dest-port destination_port ]
```

Specifies sending disconnect message.

**dest-port destination_port**: Optionally, the port number to which the disconnect message must be sent can be specified.

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

```
interim create-new-call
```

Default: disabled

Enables the ability to create a new session upon receipt of a RADIUS interim message.

**Usage**

Use this command to configure the communication with the RADIUS client from which RADIUS accounting requests are received.

**Example**

The following command configures the service to communicate with a RADIUS client with an IP address of 1.2.3.4 and an encrypted shared secret of **secret_1234**:

```
radius accounting client 1.2.3.4 encrypted key secret_1234
```
radius dictionary

Configures the RADIUS database dictionary to use for the IPSG service.

**Product**
IPSG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
radius dictionary db
```

default radius dictionary

dictionary db
Default: starent-vsa1
Specifies what dictionary database to use. The possible values for db are described in the table that follows:

**Table 26.**

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>customXX</td>
<td>These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. XX is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-835</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-vsa1</td>
<td>This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0-255). This is the default dictionary.</td>
</tr>
<tr>
<td>starent-vsa1-835</td>
<td>This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0-255). This is the default dictionary.</td>
</tr>
</tbody>
</table>
radius dictionary

Usage
Use this command to specify the RADIUS database dictionary to use for the IPSG service.

Example
The following command configures the IPSG service to use the custom10 RADIUS database dictionary:

radius dictionary custom10
setup-timeout

Configures a timeout value for IPSG session set up attempts.

**Product**
IPSG

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
setup-timeout seconds

default setup-timeout

seconds
```

Default: 60

Specifies the time period, in seconds, the IPSG session setup is allowed to continue before the set up attempt is terminated. `seconds` must be an integer from 1 through 100000.

**Usage**

Use this command to prevent IPSG session set up attempts from continuing without termination.

**Example**

The following command sets the session set up timeout to 20 seconds:

```plaintext
setup-timeout 20
```
Chapter 133
IPSG RADIUS Snoop Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Snoop Configuration Mode is used to create and configure IPSG services within the current system context. The IPSG RADIUS Snoop Mode configures the system to inspect RADIUS accounting requests on the way to the RADIUS accounting server and extract user information.

```
Exec Mode
configure
Global Configuration Mode
context name
Context Configuration Mode
ipsg-service name mode radius-snoop
IPSG RADIUS Snoop Config Mode
```

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

Configures the service to accept data on any interface configured in the context. Optionally allows the system to limit the number of sessions processed by this service.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

bind [ max-subscribers num ]

no bind

no
Removes the binding for the service.

max-subscribers num

Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.
In Release 8.x, on an ASR 5000 chassis, num must be an integer from 0 through 3000000.
In Release 9.0 and later, num must be an integer from 0 through 4000000.

Usage
Use this command to initiate the service and begin accepting data on any interface configured in the context.

Example
The following command prepares the system to receive subscriber sessions on any interface in the context and limits the sessions to 10000:

bind max-subscribers 10000
connection authorization

Sets the RADIUS authorization password that must be matched by the RADIUS accounting requests “snooped” by this service.

**Product**
IPSG

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
connection authorization { [ encrypted ] password password }
no connection authorization
```

- **no**
  
  Removes the RADIUS authorization for the IPSG RADIUS snoop service.

- **[ encrypted ] password password**
  
  encrypted: Indicates that the received RADIUS authorization password is encrypted.
  
  password: Specifies the password that must be matched by incoming RADIUS accounting requests.
  
  password must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

RADIUS accounting requests being examined by the IPSG RADIUS snoop service are destined for a RADIUS Accounting Server. Since the “snoop” service does not terminate user authentication, the user password is unknown.

Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

**Example**

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests “snooped” by this service. The password must be encrypted and the example provided is the word “secret”.

```plaintext
connection authorization encrypted password secret
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec Mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

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

Specifies RADIUS Accounting Servers where accounting requests are sent after being “inspected” by this service.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

[ no ] radius { accounting server address [ port num | source-context name ] |
dictionary { 3gpp2 | 3gpp2-835 | customXX | standard | starent | starent-835 |
starent-vsa1 | starent-vsa1-835 } }

no
Removes the RADIUS accounting server identifier from this service.

radius accounting server address

Specifies the IP address of a RADIUS Accounting Server where accounting requests are sent after being “snooped” by this service. address must be specified using standard IPv4 or IPv6 dotted decimal notation and must be a valid IP address.
Up to 16 addresses can be configured.

port num

Default: 1813
Specifies the port number of the RADIUS Accounting Server where accounting requests are sent after being “snooped” by this service.
num must be an integer from 0 through 65535.

source-context name

Specifies the source context where RADIUS accounting requests are received.
name must be an alpha and/or numeric string of 1 through 79 characters in length.
If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

dictionary { 3gpp2 | 3gpp2-835 | customXX | standard | starent |
starent-835 | starent-vsa1 | starent-vsa1-835 }

Specifies what dictionary database to use. The possible values are described in the following table:

Table 27.

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>customXX</td>
<td>These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. XX is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-835</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-vsa1</td>
<td>This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.</td>
</tr>
<tr>
<td>starent-vsa1-835</td>
<td>This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to specify the RADIUS Accounting Servers where accounting requests are sent after being snooped by this service.

**Example**

The following command specifies the IP address (1.2.3.4) of a RADIUS Accounting Server whose accounting requests are to be “snooped”, and the source context (aaa_ingress) where the requests are received on the system:

```
radius accounting server 1.2.3.4 source-context aaa_ingress
```
setup-timeout

Configures a timeout value for IPSG session setup attempts.

Product
IPSG

Privilege
Security Administrator, Administrator

Syntax

```
setup-timeout seconds

default setup-timeout

seconds

Default: 60
Specifications the period of time, in seconds, the IPSG session setup is allowed to continue before the setup attempt is terminated.

seconds must be an integer from 1 through 100000.
```

Usage
Use this command to prevent IPSG session setup attempts from continuing without termination.

Example
The following command sets the session setup timeout to 20 seconds:

```
setup-timeout 20
```
Chapter 134
IPSP Configuration Mode Commands

The IPSP Configuration Mode is used to configure properties for the IP pool sharing protocol (IPSP).

Important: For information on configuring and using IPSP refer to the System Administration and Configuration Guide.
dead-interval

Configures the retry time to connect to the remote system for the IP Pool Sharing Protocol.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

`dead-interval seconds`

`[ no | default ] dead-interval`

no
Disables the dead interval. On loss of connectivity to the remote system, no retries are attempted and the remote system is marked dead immediately on failure.

default
Resets the dead interval to the default of 3600 seconds.

seconds
Default: 3600 seconds
The amount of time in seconds to wait before retrying the remote system. `seconds` must be an integer from 25 through 259200.

Usage
Use this command to set the amount of time to wait before retrying to connect with the remote system for the IP pool sharing protocol.

Example
Use the following command to set the interval to 180 seconds (3 minutes):

dead-interval 180
end

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

**Product**
- PDSN, HA

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Return to the Exec mode.
exit

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

**Product**

PDNS, HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the context configuration mode.
reserved-free-percentage

This command is used to set the amount of free addresses reserved for use on the primary HA.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

reserved-free-percentage value

default reserved-free-percentage

value
Default: 100

value specifies the percentage of free addresses reserved for the use on the primary HA for IP pool sharing during upgrade.

Usage
This command is used with pool-sharing-protocol active mode on primary HA. Before using this command, pool-sharing-protocol in Ethernet Interface Configuration Mode must be configured.

For more information, refer to the Ethernet Interface Configuration Mode Commands chapter in this guide.

Example
To reserve 40 percent of free addresses in primary HA for IP pool sharing, enter the following command:

reserved-free-percentage 40
Chapter 135
IPv6 ACL Configuration Mode Commands

The IPv6 Access Control List Configuration Mode is used to create and manage IPv6 access privileges.
deny/permit

The following commands set access permissions based on various parameters:
deny/permit (by source IP address masking)

Used to filter subscriber sessions based on the IPv6 address mask sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
{ deny | permit } [ log ] source_address source_wildcard
after { deny | permit } [ log ] source_address source_wildcard
before { deny | permit } [ log ] source_address source_wildcard
no { deny | permit } [ log ] source_address source_wildcard
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**deny | permit**
Specifies the rule is either block (deny) or an allow (permit) filter.
**deny:** indicates the rule, when matched, drops the corresponding packets.
**permit:** indicates the rule, when matched, allows the corresponding packets.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.
deny/permit (by source IP address masking)

**source_address**

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source wildcard parameter.

**sourceWildcard**

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rules as it does not require a rule for each source and destination pair.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.
deny/permit (any)

Used to filter subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[
\text{deny/permit (any)} \quad \text{[ log ] any}
\]

\text{after (deny | permit) [ log ] any}

\text{before (deny | permit) [ log ] any}

\text{no (deny | permit) [ log ] any}

\text{after}
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

\text{Important: If the options specified do not exactly match an existing rule, the insertion point does not change.}

\text{before}
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

\text{Important: If the options specified do not exactly match an existing rule, the insertion point does not change.}

\text{no}
Removes the rule which exactly matches the options specified.

\text{deny | permit}
Specifies the rule is either block (deny) or an allow (permit) filter.
\text{deny}: indicates the rule, when matched, drops the corresponding packets.
\text{permit}: indicates the rule, when matched, allows the corresponding packets.

\text{log}
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

**any**

Indicates all packets will match the filter regardless of source and/or destination.

---

**Usage**

Define a catch all rule to place at the end of the list of rules.

---

**Important:** It is suggested that any rule which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.

---

**Example**

The following command defines two rules with the second logging filtered packets.

```
permit any deny log any
```

The following sets the insertion point to before the first rule defined above.

```
before permit any
```

The following command sets the insertion point after the second rule defined above.

```
after deny log any
```

The following deletes the first rule defined above.

```
no permit any
```
deny/permit (by host IP address)

Used to filter subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
{ deny | permit } [ log ] host source_host_address
after { deny | permit } [ log ] host source_host_address
before { deny | permit } [ log ] host source_host_address
no { deny | permit } [ log ] host source_host_address
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**deny | permit**
Specifies the rule is either block (deny) or an allow (permit) filter.
**deny**: indicates the rule, when matched, drops the corresponding packets.
**permit**: indicates the rule, when matched, allows the corresponding packets.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.
deny/permit (by source ICMP packets)

Used to filter subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
{ deny | permit } [ log ] icmp { source_address source wildcard | any |
hostsource_host_address } { dest_address dest wildcard | any |
hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

```
after { deny | permit } [ log ] icmp { source_address source wildcard | any |
hostsource_host_address } { dest_address dest wildcard | any |
hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

```
before { deny | permit } [ log ] icmp { source_address source wildcard | any |
hostsource_host_address } { dest_address dest wildcard | any |
hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

```
no { deny | permit } [ log ] icmp { source_address source wildcard | any |
hostsource_host_address } { dest_address dest wildcard | any |
hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```
no
```

Removes the rule which exactly matches the options specified.
deny | permit
Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: indicates the rule, when matched, drops the corresponding packets.
- **permit**: indicates the rule, when matched, allows the corresponding packets.

log
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

source_wildcard
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
**deny/permit (by source ICMP packets)**

- **dest_wildcard**
  
  This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

- **icmp_type**
  
  Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

- **icmp_code**
  
  Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.
deny/permit (by IP packets)

Used to filter subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

\[
\begin{align*}
\text{deny | permit | log | ip} & \{ \text{source_address source_wildcard | any} | \\
& \text{hostsource_host_address} \} \{ \text{dest_address dest_wildcard | any} | \\
& \text{hostdest_host_address} \} [ \text{fragment} | \text{protocol num} ] \\
\text{after} & \{ \text{deny | permit | log | ip} \{ \text{source_address source_wildcard | any} | \\
& \text{hostsource_host_address} \} \{ \text{dest_address dest_wildcard | any} | \\
& \text{hostdest_host_address} \} [ \text{fragment} | \text{protocol num} ] \\
\text{before} & \{ \text{deny | permit | log | ip} \{ \text{source_address source_wildcard | any} | \\
& \text{hostsource_host_address} \} \{ \text{dest_address dest_wildcard | any} | \\
& \text{hostdest_host_address} \} [ \text{fragment} | \text{protocol num} ] \\
\text{no} & \{ \text{deny | permit | log | ip} \{ \text{source_address source_wildcard | any} | \\
& \text{hostsource_host_address} \} \{ \text{dest_address dest_wildcard | any} | \\
& \text{hostdest_host_address} \} [ \text{fragment} | \text{protocol num} ] \\
\end{align*}
\]

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.
deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.
deny: indicates the rule, when matched, drops the corresponding packets.
permit: indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the sourceWildcard parameter.

sourceWildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the destWildcard parameter.
**deny/permit (by IP packets)**

**dest_wildcard**

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**fragment**

Indicates packet filtering is to be applied to IP packet fragments only.

**protocol num**

Indicates that the packet filtering is to be applied to a specific protocol number.

`num` can be any integer ranging from 0 to 255.

**Usage**

Block IP packets when the source and destination are of interest.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.
deny/permit (by TCP/UDP packets)

Used to filter subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
{ deny | permit } [ log ] { tcp | udp } { { source_address source wildcard | any | hostsource_host_address } [ eqsource_port | gtsource_port | ltsource_port | neqsource_port ] } { { dest_address dest wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port | ltdest_port | neqdest_port ] }
```

```plaintext
after { deny | permit } [ log ] { tcp | udp } { { source_address source wildcard | any | hostsource_host_address } [ eqsource_port | gtsource_port | ltsource_port | neqsource_port ] } { { dest_address dest wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port | ltdest_port | neqdest_port ] }
```

```plaintext
before { deny | permit } [ log ] { tcp | udp } { { source_address source wildcard | any | hostsource_host_address } [ eqsource_port | gtsource_host_port | ltsource_port | neqsource_port ] } { { dest_address dest wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port | ltdest_port | neqdest_port ] }
```

```plaintext
no { deny | permit } [ log ] { tcp | udp } { { source_address source wildcard | any | hostsource_host_address } [ eqsource_port | gtsource_port | ltsource_port | neqsource_port ] } { { dest_address dest wildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port | ltdest_port | neqdest_port ] }
```

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the rule which exactly matches the options specified.</td>
</tr>
<tr>
<td>deny</td>
<td>Indicates the rule, when matched, drops the corresponding packets.</td>
</tr>
<tr>
<td>permit</td>
<td>Indicates the rule, when matched, allows the corresponding packets.</td>
</tr>
<tr>
<td>log</td>
<td>Default: packets are not logged. Indicates all packets which match the filter are to be logged.</td>
</tr>
<tr>
<td>tcp</td>
<td>Applies to TCP packets.</td>
</tr>
<tr>
<td>udp</td>
<td>Applies to UDP packets.</td>
</tr>
<tr>
<td>source_address</td>
<td>The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
<tr>
<td>source_wildcard</td>
<td>This option is used in conjunction with the <code>source_address</code> option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement: - Zero-bits in this parameter mean that the corresponding bits configured for the <code>source_address</code> parameter must be identical. - One-bits in this parameter mean that the corresponding bits configured for the <code>source_address</code> parameter must be ignored.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that the rule applies to all packets.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies that the rule applies to a specific host as determined by its IP address.</td>
</tr>
</tbody>
</table>
**source_host_address**
The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv6 colon notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered. 
*source_port* must be configured to any integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered. 
*source_port* must be configured to any integer value from 0 to 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered. 
*source_port* must be configured to any integer value from 0 to 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered. 
*source_port* must be configured to any integer value from 0 to 65535.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *destWildcard* parameter.

**destWildcard**
This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**eq dest_port**
Specifies a single, specific destination TCP port number to be filtered. 
*dest_port* must be configured to any integer value from 0 to 65535.
### configure acl (by TCP/UDP packets)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gt dest_port</code></td>
<td>Specifies that all destination TCP port numbers greater than the one specified are to be filtered. <code>dest_port</code> must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td><code>lt dest_port</code></td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered. <code>dest_port</code> must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td><code>neq dest_port</code></td>
<td>Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. <code>dest_port</code> must be configured to any integer value from 0 to 65535.</td>
</tr>
</tbody>
</table>

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information.
**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.

**Example**

```
end
```
exit

Exits the ACL configuration mode and returns to the context configuration mode.

Privilege
Security Administrator, Administrator

Product
All

Syntax

```
exit
```

Usage
Return to the context configuration mode.

Example

```
exit
```
readdress server

Alter the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
readdress server
```

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```
before
```

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```
no
```

Removes the rule which exactly matches the options specified.

```
redirect_address
```

The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must be an IPv6 address specified in either : or :: notation.

```
port port_no
```

The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.

```
tcp | udp
```

Specifies the redirect is to be applied to the IP based transmission control protocol or the user datagram protocol.

tcp: redirect applies to TCP packets.

udp: redirect applies to UDP packets.
source_address
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then
be configured using the source_wildcard parameter.

any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then
be configured using the dest_wildcard parameter.

eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to any integer value from 0 to 65535.

gt dest_port
Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to any integer value from 0 to 65535.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lt dest_port</td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
</tbody>
</table>

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect context

The following commands redirect subscriber sessions to a different context based on various parameters:
redirect context (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax**

- `redirect context context_id [ log ] source_address source_wildcard`
- `after redirect context context_id [ log ] source_address source_wildcard`
- `before redirect context context_id [ log ] source_address source_wildcard`
- `noredirect context context_id [ log ] source_address source_wildcard`

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**

Removes the rule which exactly matches the options specified.

**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.
redirect context (by IP address masking)

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source wildcard parameter.

source wildcard

This option is used in conjunction with the source address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

Usage

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect context (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect context context_id [ log ] any
after redirect context context_id [ log ] any
before redirect context context_id [ log ] any
no redirect context context_id [ log ] any
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**context context_id**
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.
any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: It is suggested that any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the context with the context ID of 23 and any source IP.

```
redirect context 23 any
```

The following sets the insertion point to before the first rule defined above.

```
before redirect context 23 any
```

The following command sets the insertion point after the second rule defined above.

```
after redirect context 23 any
```

The following deletes the first rule defined above.

```
no redirect context 23 any
```
redirect context (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

redirect context context_id [ log ] host source_ip_address
after redirect context context_id [ log ] host source_ip_address
before redirect context context_id [ log ] host source_ip_address
noredirect context context_id [ log ] host source_ip_address

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**context context_id**
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.
**host**

Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon notation.

**Usage**

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect context (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect context context_id [ log ] icmp { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

```
after redirect context context_id [ log ] icmp { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

```
before redirect context context_id [ log ] icmp { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

```
no redirect context context_id [ log ] icmp { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ icmp_type [ icmp_code ] ]
```

```
  after
  Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
  This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.
```

```
  Important: If the options specified do not exactly match an existing rule, the insertion point does not change.
```

```
  before
  Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
  This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
```

```
  Important: If the options specified do not exactly match an existing rule, the insertion point does not change.
```

```
  no
  Removes the rule which exactly matches the options specified.
```
redirect context (by source ICMP packets)

context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the sourceWildcard parameter.

sourceWildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the destWildcard parameter.
**dest_wildcard**

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect context (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect context context_id [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ fragment ] [ protocol num ]

after redirect context context_id [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ fragment ] [ protocol num ]

before redirect context context_id [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdest_host_address } [ fragment ] [ protocol num ]

no redirect context context_id [ log ] ip { source_address source_wildcard | any | hostsource_host_address } { dest_address dest_wildcard | any | hostdst_host_address } [ fragment ] [ protocol num ]
```

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**

Removes the rule which exactly matches the options specified.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule applies to all packets.

**host**

Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv6 colon notation.

**dest_address**

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
dest wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
• Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
• One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

fragment
Indicates packet redirection is to be applied to IP packet fragments only.

protocol num
Indicates that the packet filtering is to be applied to a specific protocol number.
num can be any integer ranging from 0 to 255.

Usage
Block IP packets when the source and destination are of interest.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect context (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
redirect context context_id [ log ] { tcp | udp } { { source_address
gtsource_port | ltsource_port | neqsource_port } } { { dest_address
destWildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | neqdest_port ] }

after redirect context context_id [ log ] { tcp | udp } { { source_address
gtsource_port | ltsource_port | neqsource_port } } { { dest_address
destWildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | neqdest_port ] }

before redirect context context_id [ log ] { tcp | udp } { { source_address
gtsource_port | ltsource_port | neqsource_port } } { { dest_address
destWildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | neqdest_port ] }

noredirect context context_id [ log ] { tcp | udp } { { source_address
gtsource_port | ltsource_port | neqsource_port } } { { dest_address
defstWildcard | any | hostdest_host_address } [ eqdest_port | gtdest_port |
ltdest_port | neqdest_port ] }
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **context context_id**
  The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **tcp | udp**
  Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
  - `tcp`: redirect applies to TPC packets.
  - `udp`: redirect applies to UDP packets.

- **source_address**
  The IP address(es) form which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

- **source_wildcard**
  This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

- **any**
  Specifies that the rule applies to all packets.

- **host**
  Specifies that the rule applies to a specific host as determined by its IP address.
IPv6 ACL Configuration Mode Commands

**source_host_address**
The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv6 colon notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
*source_port* must be configured to any integer value from 0 to 65535.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *destWildcard* parameter.

**destWildcard**
This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**eq dest_port**
Specifies a single, specific destination TCP port number to be filtered.
*dest_port* must be configured to any integer value from 0 to 65535.
**redirect context (by TCP/UDP packets)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gt dest_port</code></td>
<td>Specifies that all destination TCP port numbers greater than the one specified are to be filtered. <code>dest_port</code> must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td><code>lt dest_port</code></td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered. <code>dest_port</code> must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td><code>neq dest_port</code></td>
<td>Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. <code>dest_port</code> must be configured to any integer value from 0 to 65535.</td>
</tr>
</tbody>
</table>

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23, and UDP packets coming from any host are matched.

```
redirect context 23 udp any
```

The following sets the insertion point to before the rule defined above.

```
before redirect context 23 udp any
```

The following command sets the insertion point after the rule defined above.

```
after redirect context 23 udp any
```

The following deletes the rule defined above.

```
no redirect context 23 udp any
```
redirect css delivery-sequence

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.
redirect css service

The following commands redirect subscriber sessions to Content Service Steering (CSS) services based on various parameters:
**redirect css service (any)**

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[ log] any
before redirect css service svc_name[ log] any
after redirect css service svc_name[ log] any
no redirect css service svc_name[ log] any
```

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definitions which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`svc_name` must be a string of 1 through 15 characters in length.

**log**
Default: packets are not logged.
redirect css service (any)

Indicates all packets which match the redirect are to be logged.

any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important**: It is suggested that any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important**: A maximum of 16 rule definitions can be configured per ACL.

**Important**: Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule definition that redirects packets to the charging service with the name `chgsvc1` and any source IP.

```
redirect css service chgsvc1 any
```

The following sets the insertion point to before the first rule definition above.

```
before redirect service chgsvc1 any
```

The following command sets the insertion point after the second rule definitions above.

```
after redirect service chgsvc1 any
```

The following deletes the first rule definition above.

```
no redirect service chgsvc1 any
```
**redirect css service (by host IP address)**

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[ log ] host source_host_address
before redirect css service svc_name[ log ] host source_host_address
after redirect css service svc_name[ log ] host source_host_address
no redirect css service svc_name[ log ] host source_host_address
```

- **after**
  Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
  This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

- **Important**: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **before**
  Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
  This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

- **Important**: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **no**
  Removes the rule definition which exactly matches the options specified.

- **css service svc_name**
  The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
  `svc_name` must be a string of 1 through 15 characters in length.

- **log**
  Default: packets are not logged.
redirect css service (by host IP address)

Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon notation.

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect css service (by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
redirect css service svc_name[log]icmp {any|host source_host_address|source_address source_wildcard}{any|host dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]]
before redirect css service svc_name[log]icmp {any|host source_host_address|source_address source_wildcard}{any|host dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]]
after redirect css service svc_name[log]icmp {any|host source_host_address|source_address source_wildcard}{any|host dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]]
no redirect css service svc_name[log]icmp {any|host source_host_address|source_address source_wildcard}{any|host dest_host_address|dest_address dest_wildcard}[icmp_type[icmp_code]]
```

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.
**css service svc_name**  
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.  
`svc_name` must be a string of 1 through 15 characters in length.

**log**  
Default: packets are not logged.  
Indicates all packets which match the redirect are to be logged.

**source_address**  
The IP address(es) form which the packet originated.  
This option is used to filter all packets from a specific IP address or a group of IP addresses.  
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source wildcard` parameter.

**source wildcard**  
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.  
The mask must be entered as a complement:  
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.  
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**  
Specifies that the rule definition applies to all packets.

**host**  
Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**  
The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**  
The IP address of the destination host to filter against expressed in IPv6 colon notation.

**dest_address**  
The IP address(es) to which the packet is to be sent.  
This option is used to filter all packets to a specific IP address or a group of IP addresses.  
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest wildcard` parameter.
IPv6 ACL Configuration Mode Commands

**redirect css service (by ICMP packets)**

`dest_wildcard`

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- **Zero-bits** in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- **One-bits** in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

`icmp_type`

Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

`icmp_code`

Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

**Usage**

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
**redirect css service (by IP packets)**

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
before redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
after redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
no redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. *svc_name* must be a string of 1 through 15 characters in length.

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

Note: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

Specifies that the rule definition applies to all packets.

Specifies that the rule definition applies to a specific host as determined by its IP address.

The IP address of the source host to filter against expressed in IPv6 colon notation.

The IP address of the destination host to filter against expressed in IPv6 colon notation.

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
**destWildcard**

This option is used in conjunction with the `destAddress` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `destAddress` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `destAddress` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**fragment**

Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**

Block IP packets when the source and destination are of interest.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect css service (by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service svc_name[log]source_address source_wildcard
before redirect css service svc_name[log]source_address source_wildcard
after redirect css service svc_name[log]source_address source_wildcard
no redirect css service svc_name[log]source_address source_wildcard
```

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.

**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`svc_name` must be a string of 1 through 15 characters in length.

**log**

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.
**redirect css service (by source IP address masking)**

<table>
<thead>
<tr>
<th>source_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>source_wildcard</th>
</tr>
</thead>
</table>
| This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:  
  • Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.  
  • One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored. |

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**Usage**

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Example**

The following command defines a rule definition to redirect packets to a charging service named `chgsvc1`.

```
redirect css service chgsvc1 1:1:1:1:1:1:1
```
redirect css service (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by
the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service svc_name[log]{tcp|udp}{ {source_address
source_wildcard|any|host source_host_address}{eq source_port|gt
source_port|lt source_port|neq source_port|range start source_port
end source_port}} { {dest_address dest_wildcard|any|host dest_host_address
} {eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start dest_port
end dest_port}}
```

```
before redirect css service svc_name[log]{tcp|udp}{ {source_address
source_wildcard|any|host source_host_address}{eq source_port|gt
source_port|lt source_port|neq source_port|range start source_port
end source_port}} { {dest_address dest_wildcard|any|host dest_host_address
} {eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start dest_port
end dest_port}}
```

```
amo redirect css service svc_name[log]{tcp|udp}{ {source_address
source_wildcard|any|host source_host_address}{eq source_port|gt
source_port|lt source_port|neq source_port|range start source_port
end source_port}} { {dest_address dest_wildcard|any|host dest_host_address
} {eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start dest_port
end dest_port}}
```

```
before
```

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by
the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options
specified such that new rule definitions will be added, in order, after the matching rule definition.

```
Important: If the options specified do not exactly match an existing rule definition, the insertion point does not
change.
```

```
after
```

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by
the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

- **svc_name** must be a string of 1 through 15 characters in length.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**tcp | udp**
Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: redirect applies to TCP packets.
- **udp**: redirect applies to UDP packets.

**source_address**
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source wildcard` parameter.

**source wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**
Specifies that the rule definition applies to all packets.
**host**
Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv6 colon notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered. 
`source_port` must be configured to any integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
`source_port` must be configured to any integer value from 0 to 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered.
`source_port` must be configured to any integer value from 0 to 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered. 
`source_port` must be configured to any integer value from 0 to 65535.

**range start_source_port end_source_port**
Specifies that all source TCP ports within a specific range are to be filtered.
`start_source_port` is the initial port in the range and `end_source_port` is the final port in the range. 
Both `start_source_port` and `end_source_port` can be configured to any integer value from 0 to 65535.

**dest_address**
The IP address(es) to which the packet is to be sent. 
This option is used to filter all packets to a specific IP address or a group of IP addresses. 
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

**dest_wildcard**
This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. 
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Value Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq dest_port</td>
<td>Specifies a single, specific destination TCP port number to be filtered.</td>
<td>dest_port</td>
</tr>
<tr>
<td></td>
<td>dest_port must be configured to any integer value from 0 to 65535.</td>
<td></td>
</tr>
<tr>
<td>gt dest_port</td>
<td>Specifies that all destination TCP port numbers greater than the one specified are to be filtered.</td>
<td>dest_port</td>
</tr>
<tr>
<td></td>
<td>dest_port must be configured to any integer value from 0 to 65535.</td>
<td></td>
</tr>
<tr>
<td>lt dest_port</td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered.</td>
<td>dest_port</td>
</tr>
<tr>
<td></td>
<td>dest_port must be configured to any integer value from 0 to 65535.</td>
<td></td>
</tr>
<tr>
<td>neq dest_port</td>
<td>Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.</td>
<td>dest_port</td>
</tr>
<tr>
<td></td>
<td>dest_port must be configured to any integer value from 0 to 65535.</td>
<td></td>
</tr>
<tr>
<td>range start_dest_port end_dest_port</td>
<td>Specifies that all destination TCP ports within a specific range are to be filtered.</td>
<td>start_dest_port</td>
</tr>
<tr>
<td></td>
<td>end_dest_port is the initial port in the range and end_dest_port is the final port in the range.</td>
<td>end_dest_port</td>
</tr>
<tr>
<td></td>
<td>Both start_dest_port and end_dest_port can be configured to any integer value from 0 to 65535.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service named `chgsvc1`, and UDP packets coming from any host are matched.
```
redirect css service chgsvc1 udp any
```
The following sets the insertion point to before the rule definition above.
```
before redirect css service chgsvc1 udp any
```
The following command sets the insertion point after the rule definition above.
```
after redirect css service chgsvc1 udp any
```
The following deletes the rule definition above.
```
no redirect css service chgsvc1 udp any
```
redirect css service (for downlink, any)

Used to redirect subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
redirect css service svc_name[ log]downlink any
before redirect css service svc_name[ log]downlink any
after redirect css service svc_name[ log]downlink any
no redirect css service svc_name[ log]downlink any
```

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
`svc_name` must be a string of 1 through 15 characters in length.

**downlink**
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.
**redirect css service (for downlink, any)**

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**any**
Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**
Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service with the name chgsvcl and any source IP.

```
redirect css service chgsvcl downlink any
```

The following sets the insertion point to before the first rule definition above.

```
before redirect service chgsvcl downlink any
```

The following command sets the insertion point after the second rule definition above.

```
after redirect service chgsvcl downlink any
```

The following deletes the first rule definition above.

```
no redirect service chgsvcl downlink any
```
redirect css service (for downlink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
redirect css service svc_name[log]downlink host source_host_address
before redirect css service svc_name[log]downlink host
source_host_address
after redirect css service svc_name[log]downlink host source_host_address
no redirect css service svc_name[log]downlink host source_host_address
```

- **before**
  - Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
  - This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

  **Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **after**
  - Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
  - This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

  **Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **no**
  - Removes the rule definition which exactly matches the options specified.

- **css service svc_name**
  - The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
  - `svc_name` must be a string of 1 through 15 characters in length.
redirect css service (for downlink, by host IP address)

**downlink**
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**host**
Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv6 colon notation.

**Usage**
Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important**: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect css service (for downlink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service svc_name[ log] downlink icmp { any | host
source_host_address| source_address source wildcard} | any | host
dest_host_address| dest_address dest wildcard}[ icmp_type| icmp_code]
```

```
before redirect css service svc_name[ log] downlink icmp { any | host
source_host_address| source_address source wildcard} | any | host
dest_host_address| dest_address dest wildcard}[ icmp_type| icmp_code]
```

```
after redirect css service svc_name[ log] downlink icmp { any | host
source_host_address| source_address source wildcard} | any | host
dest_host_address| dest_address dest wildcard}[ icmp_type| icmp_code]
```

```
o redirect css service svc_name[ log] downlink icmp { any | host
source_host_address| source_address source wildcard} | any | host
dest_host_address| dest_address dest wildcard}[ icmp_type| icmp_code]
```

---

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

---

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

**no**

Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string of 1 through 15 characters in length.

**downlink**

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**

Specifies that the rule definition applies to all packets.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv6 colon notation.
IPv6 ACL Configuration Mode Commands

redirect css service (for downlink, by ICMP packets)

---

**dest_address**

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

---

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

---

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

---

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

---

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

---

**Usage**

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

---

**Important**: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect css service (for downlink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service svc_name [log] downlink ip {any | host
source_host_address | source_address source_wildcard}
{any | host
derest_host_address | dest_address dest_wildcard} [fragment]
before redirect css service svc_name [log] downlink ip {any | host
source_host_address | source_address source_wildcard}
{any | host
derest_host_address | dest_address dest_wildcard} [fragment]
after redirect css service svc_name [log] downlink ip {any | host
source_host_address | source_address source_wildcard}
{any | host
derest_host_address | dest_address dest_wildcard} [fragment]
no redirect css service svc_name [log] downlink ip {any | host
source_host_address | source_address source_wildcard}
{any | host
derest_host_address | dest_address dest_wildcard} [fragment]
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

---

IPv6 ACL Configuration Mode Commands
**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string of 1 through 15 characters in length.

**downlink**
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**source_address**
The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**
Specifies that the rule definition applies to all packets.

**host**
Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv6 colon notation.
redirect css service (for downlink, by IP packets)

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `destWildcard` parameter.

**destWildcard**
This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**fragment**
Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**
Block IP packets when the source and destination are of interest.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect css service (for downlink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[log]downlink source_address source_wildcard
before redirect css service svc_name[log]downlink source_address source_wildcard
after redirect css service svc_name[log]downlink source_address source_wildcard
no redirect css service svc_name[log]downlink source_address source_wildcard
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
redirect css service (for downlink, by source IP address masking)

svc_name must be a string of 1 through 15 characters in length.

downlink
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

Usage
Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

Example
The following command defines a rule definition to redirect packets to a charging service named chgsvc1.

```
redirect css service chgsvc1 downlink 1:1:1:1:1:1:1
```
redirect css service (for downlink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[ log]downlink { tcp|udp } { { source_address
source_wildcard|any|host source_host_address} [eq source_port|gt
source_port|lt source_port|neq source_port|range start_source_port
end_source_port]} { { dest_address dest_wildcard|any|host dest_host_address
} [eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port
end_dest_port]}
```

**before redirect css service svc_name[ log]downlink { tcp|udp } { { source_address
source_wildcard|any|host source_host_address} [eq source_port|gt
source_port|lt source_port|neq source_port|range start_source_port
end_source_port]} { { dest_address dest_wildcard|any|host dest_host_address
} [eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port
end_dest_port]}

**after redirect css service svc_name[ log]downlink { tcp|udp } { { source_address
source_wildcard|any|host source_host_address} [eq source_port|gt
source_port|lt source_port|neq source_port|range start_source_port
end_source_port]} { { dest_address dest_wildcard|any|host dest_host_address
} [eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port
end_dest_port]}

**no redirect css service svc_name[ log]downlink { tcp|udp } { { source_address
source_wildcard|any|host source_host_address} [eq source_port|gt
source_port|lt source_port|neq source_port|range start_source_port
end_source_port]} { { dest_address dest_wildcard|any|host dest_host_address
} [eq dest_port|gt dest_port|lt dest_port|neq dst_port|range start_dest_port
end_dest_port]}

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```no```
Removes the rule definition which exactly matches the options specified.

```css service svc_name```
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string of 1 through 15 characters in length.

```downlink```
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

```log```
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

```tcp | udp```
Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
- `tcp`: redirect applies to TCP packets.
- `udp`: redirect applies to UDP packets.

```source_address```
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

```source_wildcard```
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- • Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- • One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.
any
Specifies that the rule definition applies to all packets.

host
Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

range start_source_port end_source_port
Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and end_source_port is the final port in the range.
Both start_source_port and end_source_port can be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
IPv6 ACL Configuration Mode Commands

- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq dest_port</td>
<td>Specifies a single, specific destination TCP port number to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td>gt dest_port</td>
<td>Specifies that all destination TCP port numbers greater than the one specified are to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td>lt dest_port</td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td>neq dest_port</td>
<td>Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. dest_port must be configured to any integer value from 0 to 65535.</td>
</tr>
<tr>
<td>range start_dest_port end_dest_port</td>
<td>Specifies that all destination TCP ports within a specific range are to be filtered. start_dest_port is the initial port in the range and end_dest_port is the final port in the range. Both start_dest_port and end_dest_port can be configured to any integer value from 0 to 65535.</td>
</tr>
</tbody>
</table>

**Usage**
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service named chgsvc1, and UDP packets coming from any host are matched.

```
redirect css service chgsvc1 downlink udp any
```
The following sets the insertion point to before the rule definition above.

```
before redirect css service chgsvc1 downlink udp any
```
The following command sets the insertion point after the rule definition above.

```
after redirect css service chgsvc1 downlink udp any
```
The following deletes the rule definition above.
no redirect css service chgsvc1downlink udp any
redirect css service (for uplink, any)

Used to redirect subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name [log] uplink any
before redirect css service svc_name [log] uplink any
after redirect css service svc_name [log] uplink any
no redirect css service svc_name [log] uplink any
```

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.

**css service svc_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
`svc_name` must be a string of 1 through 15 characters in length.

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.
IPv6 ACL Configuration Mode Commands

**redirect css service** (for uplink, any)

### log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

### any
Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**
Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service with the name `chgsvc1` and any source IP.

```
redirect css service chgsvc1 uplink any
```

The following sets the insertion point to before the first rule definition above.

```
before redirect css service chgsvc1 uplink any
```

The following command sets the insertion point after the second rule definition above.

```
after redirect css service chgsvc1 uplink any
```

The following deletes the first rule definition above.

```
no redirect css service chgsvc1 uplink any
```
redirect css service (for uplink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name[log] uplink host source_host_address
before redirect css service svc_name[log] uplink host source_host_address
after redirect css service svc_name[log] uplink host source_host_address
no redirect css service svc_name[log] uplink host source_host_address
```

**uplink**
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string of 1 through 15 characters in length.
IPv6 ACL Configuration Mode Commands

redirect css service (for uplink, by host IP address)

---

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

---

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

---

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

---

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon notation.

---

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

---

**Important**: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect css service (for uplink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name [log] uplink icmp {any | host
source_host_address | source_address source wildcard} {any | host
dest_host_address | dest_address dest wildcard} [icmp_type [icmp_code]
before redirect css service svc_name [log] uplink icmp {any | host
source_host_address | source_address source wildcard} {any | host
dest_host_address | dest_address dest wildcard} [icmp_type [icmp_code]
after redirect css service svc_name [log] uplink icmp {any | host
source_host_address | source_address source wildcard} {any | host
dest_host_address | dest_address dest wildcard} [icmp_type [icmp_code]
no redirect css service svc_name [log] uplink icmp {any | host
source_host_address | source_address source wildcard} {any | host
dest_host_address | dest_address dest wildcard} [icmp_type [icmp_code]
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
css service svc_name

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the show active-charging service all command to display the names of all configured charging services.

svc_name must be a string of 1 through 15 characters in length.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source wildcard parameter.

source_wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.
IPv6 ACL Configuration Mode Commands

redirect css service (for uplink, by ICMP packets)

---

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

---

**dest_wildcard**

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

---

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.

---

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.

---

**Usage**

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect css service (for uplink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

```
before redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

```
after redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

```
no redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string of 1 through 15 characters in length.

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

Specifies that the rule definition applies to all packets.

Specifies that the rule definition applies to a specific host as determined by its IP address.

The IP address of the source host to filter against expressed in IPv6 colon notation.

The IP address of the destination host to filter against expressed in IPv6 colon notation.
**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

**dest_wildcard**

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**fragment**

Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**

Block IP packets when the source and destination are of interest.
redirect css service (for uplink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect css service <svc_name> [log] uplink <source_address> <source_wildcard>
before redirect css service <svc_name> [log] uplink <source_address> <source_wildcard>
after redirect css service <svc_name> [log] uplink <source_address> <source_wildcard>
no redirect css service <svc_name> [log] uplink <source_address> <source_wildcard>
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**no**
Removes the rule definition which exactly matches the options specified.

**css service <svc_name>**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `svc_name` must be a string of 1 through 15 characters in length.

**uplink**
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**
Default: packets are not logged. Indicates all packets which match the filter are to be logged.
source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Example

The following command defines a rule definition to redirect packets to a charging service named chgsvcl.

```
redirect css service chgsvcl uplink 1:1:1:1:1:1:1:1
```
redirect css service (for uplink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
redirect css service svc_name[log] uplink { tcp|udp } {{ source_address source_port|neq source_port|range start_source_port end_source_port} {{ dest_address dest_port|eq dest_port|lt dest_port|lt dest_port|neq dest_port|range start_dest_port end_dest_port}}
before redirect css service svc_name[log] uplink { tcp|udp } {{ source_address source_port|neq source_port|range start_source_port end_source_port} {{ dest_address dest_wildcard|any|host dest_host_address} [ eq dest_port|gt dest_port|lt dest_port|neq dest_port|range start_dest_port end_dest_port]}
after redirect css service svc_name[log] uplink { tcp|udp } {{ source_address source_port|neq source_port|gt source_port|lt source_port|neq source_port|range start_source_port end_source_port} {{ dest_address dest_wildcard|any|host dest_host_address} [ eq dest_port|gt dest_port|lt dest_port|neq dest_port|range start_dest_port end_dest_port]}
no redirect css service svc_name[log] uplink { tcp|udp } {{ source_address source_port|neq source_port|range start_source_port end_source_port} {{ dest_address dest_wildcard|any|host dest_host_address} [ eq dest_port|gt dest_port|lt dest_port|neq dest_port|range start_dest_port end_dest_port]}
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**no**
Removes the rule definition which exactly matches the options specified.
IPv6 ACL Configuration Mode Commands

redirect css service (for uplink, by TCP/UDP packets)

```plaintext
css service svc_name
```

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. 

- `svc_name` must be a string of 1 through 15 characters in length.

```plaintext
uplink
```

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

```plaintext
log
```

Default: packets are not logged.

- Indicates all packets which match the redirect are to be logged.

```plaintext
tcp | udp
```

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- `tcp`: redirect applies to TPC packets.
- `udp`: redirect applies to UDP packets.

```plaintext
source_address
```

The IP address(es) form which the packet originated.

- This option is used to filter all packets from a specific IP address or a group of IP addresses.
- When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

```plaintext
source_wildcard
```

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.

- The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

```plaintext
any
```

Specifies that the rule definition applies to all packets.

```plaintext
host
```

Specifies that the rule definition applies to a specific host as determined by its IP address.

```plaintext
source_host_address
```

The IP address of the source host to filter against expressed in IPv6 colon notation.

```plaintext
dest_host_address
```

The IP address of the destination host to filter against expressed in IPv6 colon notation.
eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to any integer value from 0 to 65535.

range start_source_port end_source_port
Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and end_source_port is the final port in the range.
Both start_source_port and end_source_port can be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to any integer value from 0 to 65535.

gt dest_port
Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to any integer value from 0 to 65535.
IPv6 ACL Configuration Mode Commands

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

*dest_port* must be configured to any integer value from 0 to 65535.

**neq dest_port**

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

*dest_port* must be configured to any integer value from 0 to 65535.

**range start_dest_port end_dest_port**

Specifies that all destination TCP ports within a specific range are to be filtered.

*start_dest_port* is the initial port in the range and *end_dest_port* is the final port in the range.

Both *start_dest_port* and *end_dest_port* can be configured to any integer value from 0 to 65535.

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Example**

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched.

```
redirect css service chgsvc1 uplink udp any
```

The following sets the insertion point to before the rule definition above.

```
before redirect css service chgsvc1 uplink udp any
```

The following command sets the insertion point after the rule definition above.

```
after redirect css service chgsvc1 uplink udp any
```

The following deletes the rule definition above.

```
no redirect css service chgsvc1 uplink udp any
```
redirect nexthop

The following commands redirect subscriber sessions to a nexthop IP address based on various parameters:
redirect next-hop (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
redirect next-hop next-hop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard
```

```plaintext
after redirect next-hop next-hop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard
```

```plaintext
before redirect next-hop next-hop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard
```

```plaintext
no redirect next-hop next-hop_addr { context context_id | interface interface_name } [ log ] source_address source_wildcard
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

```plaintext
next-hop next-hop_addr
```
The IP address to which the IP packets are redirected.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**interface interface_name**

The name of the logical interface to which the packets should be redirected. `interface_name` must be an alpha and/or numeric string from 1 to 79 characters in length.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect nexthop (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product
All

Privilege
Security Administrator, Administrator

Syntax

redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

nexthop nexthop_addr
The IP address to which the IP packets are redirected.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**interface interface_name**

The name of the logical interface to which the packets should be redirected. `interface_name` must be an alpha and/or numeric string from 1 to 79 characters in length.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

### Usage

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

**Important:** It is suggested that any rule which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect next-hop (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect next-hop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

```
after redirect next-hop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

```
before redirect next-hop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

```
noredirect next-hop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```
after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.
```

```
before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```
nore
Removes the rule which exactly matches the options specified.
```

```
nexthop nexthop_addr
The IP address to which the IP packets are redirected.
```
**IPv6 ACL Configuration Mode Commands**

**redirect nexthop (by host IP address)**

```
context context_id
```

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

```
interface interface_name
```

The name of the logical interface to which the packets should be redirected. **interface_name** must be an alpha and/or numeric string from 1 to 79 characters in length.

```
log
```

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

```
host
```

Specifies that the rule applies to a specific host as determined by its IP address.

```
source_host_address
```

The IP address of the source host to filter against expressed in IPv6 colon notation.

**Usage**

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect nexthop (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source wildcard | any | host source_host_address } { dest_address dst wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
after redirect interface_name nexthop_addr nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source wildcard | any | host source_host_address } { dest_address dst wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source wildcard | any | host source_host_address } { dest_address dst wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source wildcard | any | host source_host_address } { dest_address dst wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
redirect nexthop (by source ICMP packets)

For redirect nexthop commands, the rule which exactly matches the options specified.

**nexthop** nexthop_addr
The IP address to which the IP packets are redirected.

**context** context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

**interface** interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alpha and/or numeric string from 1 to 79 characters in length.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

**source_wildcard**
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**
Specifies that the rule applies to all packets.

**host**
Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv6 colon notation.
IPv6 ACL Configuration Mode Commands

```
dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.
```

```
dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
```

```
dest_wildcard
This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.
```

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

```
icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be any integer value between 0 and 255.
```

```
icmp_code
Specifies that all ICMP packets of a particular code are to be filtered. The type can be any integer value between 0 and 255.
```

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect nexthop (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
redirect nexthop (by IP packets)

- **`no`**
  Removes the rule which exactly matches the options specified.

- **`nexthop nexthop_addr`**
  The IP address to which the IP packets are redirected.

- **`context context_id`**
  The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

- **`interface interface_name`**
  The name of the logical interface to which the packets should be redirected. `interface_name` must be an alpha and/or numeric string from 1 to 79 characters in length.

- **`log`**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **`source_address`**
  The IP address(es) form which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

- **`source_wildcard`**
  This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

- **`any`**
  Specifies that the rule applies to all packets.

- **`host`**
  Specifies that the rule applies to a specific host as determined by its IP address.

- **`source_host_address`**
  The IP address of the source host to filter against expressed in IPv6 colon notation.
redirect nexthop (by IP packets)

`dest_host_address`
The IP address of the destination host to filter against expressed in IPv6 colon notation.

`dest_address`
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `destWildcard` parameter.

`destWildcard`
This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

`fragment`
Indicates packet redirection is to be applied to IP packet fragments only.

`protocol num`
Indicates that the packet filtering is to be applied to a specific protocol number. `num` can be any integer ranging from 0 to 255.

**Usage**
Block IP packets when the source and destination are of interest.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect nexthop (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source wildcard | any | host source_host_address | eq source_port | gt source_port | lt source_port | neq source_port } } { { dest_address dest wildcard | any | host dest_host_address | eq dest_port | gt dest_port | lt dest_port | neq dest_port } }
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
redirect nexthop (by TCP/UDP packets)

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **nexthop** *nexthop_addr*
  The IP address to which the IP packets are redirected.

- **context** *context_id*
  The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

- **interface** *interface_name*
  The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters in length.

- **log**
  Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

- **tcp | udp**
  Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
  - **tcp**: redirect applies to TPC packets.
  - **udp**: redirect applies to UDP packets.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

- **source_wildcard**
  This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.
any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered. source_port must be configured to any integer value from 0 to 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered. source_port must be configured to any integer value from 0 to 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered. source_port must be configured to any integer value from 0 to 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered. source_port must be configured to any integer value from 0 to 65535.

dest_address
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the destWildcard parameter.

destWildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

- **eq dest_port**
  Specifies a single, specific destination TCP port number to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

- **gt dest_port**
  Specifies that all destination TCP port numbers greater than the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

- **lt dest_port**
  Specifies that all destination TCP port numbers less than the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

- **neq dest_port**
  Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. `dest_port` must be configured to any integer value from 0 to 65535.

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. Refer to the Engineering Rules appendix located in the Administration and Configuration Guide for more information. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
The IPv6 to IPv4 Tunnel Interface Configuration Mode is used to create and manage the IP interfaces for addresses, address resolution options, etc.

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
redirect nexthop (by TCP/UDP packets)
**destination address**

Configures the destination of the tunneled packets for a manual tunnel.

**Product**
- All

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
destination address address
no destination
```

```
no
```

Removes configuration for the specified keyword.

```
text
```

Specifies the descriptive text to use. `text` must be 0 to 79 alpha and/or numeric characters with no spaces or a quoted string of printable characters

**Usage**

Set the description to provide useful information on the interface’s primary function, services, end users, etc. Any information useful may be provided.

**Example**

```
description sampleInterfaceDescriptiveText
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

   end

Usage

Change the mode back to the Exec mode.
exit

Exits the Interface Configuration Mode and returns to the Context Configuration Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
mode

Configures the mode of IPv6 to IPv4 tunneling. The default is set to manual mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
mode ( 6to4 | manual )
default mode
```

- **6to4**
  Configures automatic 6to4 IPv6 to IPv4 tunnels as specified in RFC 3056.

- **manual**
  Configures point-to-point manual IPv6 to IPv4 tunnels by specifying IPv4 address of the tunnel remote end.

- **default**
  Resets the mode of IPv6 to IPv4 tunneling to manual mode.

Usage
There can be only one 6to4 tunnel possible in a context. Once a 6to4 tunnel is configured, all subsequent tunnels will be configured as manual tunnels.

Example
The following command configures the mode to 6to4.

```
mode 6to4
```

The following command configures the mode to 6to4.

```
mode manual
```
source

Configures the source of tunneled packets.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
source { address ip_address |interface interface_name }
```

```
no source
```

- **address ip_address**
  - Specifies the IPv4 address to use as the source address of the tunnel.
  - ip_address is the IP address in dotted-decimal notation.

- **interface interface_name**
  - Specifies the name of a non-tunnel IPv4 interface, whose address is used as the source address of the tunnel.

- **no**
  - Removes configuration for the specified keyword.

Usage

Configures the source IPv4 address of the tunnel by either specifying the IP address (host address) or by specifying another configured non-tunnel IPv4 interface. The source address must be an existing interface address before it is used. State of source address will affect the operational state of the tunnel.

Example

The following command configures the source address of the tunnel.
```
source address 1.2.3.4
```

The following command specifies the source interface as testsourcel.
```
source interface testsourcel
```
tos

Configures the type of service (TOS) settings of the outer IPv4 header of the tunneled packets.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

tos {copy | value tos_value }

default tos

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>Copies the DC octet of IPv6 packet to the TOS octet of IPv4 packet.</td>
</tr>
<tr>
<td>default</td>
<td>Configures default setting for the specified keyword.</td>
</tr>
<tr>
<td>value</td>
<td>Configures the raw TOS value ranging from 0 to 255. The default is 0.</td>
</tr>
</tbody>
</table>

Usage
Sets the TOS parameter to be used in the tunnel transport protocol or instructs to copy TOS value from the original IPv6 DC byte to the TOS value of the encapsulating IPv4 header.

Example
The following command sets the tos value to 1:

tos value 1
**ttl**

Configures the TTL (Time to live) value of the outer IPv4 header of the tunneled packets.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**
```
ttl value ttl_value
```

- **default**
  Configures default setting for the specified keyword.

- **value**
  `value` is a range from 1 to 255. The default is 16.

**Usage**
Configures the TTL parameter to be used in the tunnel transport protocol.

**Example**
The following command sets the TTL value to 25.
```
ttl value 25
```
Chapter 137
ISAKMP Configuration Mode Commands

The ISAKMP Configuration Mode is used to configure Internet Security Association Key Management Protocol (ISAKMP) policies that are used to define Internet Key Exchange (IKE) security associations (SAs).

Modification(s) to an existing ISAKMP policy configuration will not take effect until the related security association has been cleared. Refer to the clear crypto security-association command located in the Exec Mode Commands chapter of the Command Line Interface Reference for more information.

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

Configures the ISAKMP policy authentication mode.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
authentication preshared-key
[ default | no ] authentication
```

**default**
Restores the default setting of this parameter. The command is enabled by default.

**no**
Disables the preshared key authentication mode.

**preshared-key**
Specifies that the policy will be authenticated through the use of the pre-shared key.

Usage
When the system is configured to use ISAKMP-type crypto maps for establishing IPSec tunnels, this command is used to indicate that the policy will be authenticated through the use of the pre-shared key configured in the ISAKMP crypto map.

Example
The following command sets policy authentication mode to use a pre-shared key:

```
authentication preshared-key
```
encryption

Configures the encryption protocol to use to protect subsequent IKE SA negotiations.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
encryption { 3des-cbc | des-cbc }
[ default | no ] encryption
```

- **default**
  Restores the default setting of this parameter.

- **no**
  Removes a previously configured encryption type.

- **3des-cbc**
  Specifies that the encryption protocol is Triple Data Encryption Standard (3DES) in chain block (CBC) mode.

- **des-cbc**
  Specifies that the encryption protocol is DES in CBC mode. This is the default setting.

Usage

Once the D-H exchange between the system and the security gateway has been successfully completed, subsequent IKE SA negotiations will be protected using the protocol specified by this command.

Example

The following command sets the IKE encryption method to 3des-cbc.

```
encryption 3des-cbc
```
**end**

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

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Returns to the Exec mode.
**exit**

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

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```bash
exit
```

**Usage**
Return to the Context Configuration mode.
### group

Configures the Oakley group (also known as the Diffie-Hellman (D-H) group) in which the D-H exchange occurs.

#### Product
PDSN, HA, GGSN

#### Privilege
Security Administrator, Administrator

#### Syntax

```
[ default | no ] group

default
Restores the default setting of this parameter.

no
Removes a previously configured group.

{ 1 | 2 | 5 }

Default: 1
The number of the Oakley group. The following groups are allowed:

- **1**: Enables Oakley Group 1 using a 768-bit modp as defined in RFC 2409.
- **2**: Enables Oakley Group 2, using a 1024-bit modp as defined in RFC 2409.
- **5**: Enables Oakley Group 5, using a 1536-bit modp as defined in RFC 3526.

#### Usage
Specifies the Oakley group that determine the length of the base prime numbers that are used during the key exchange process.

#### Example
The following command sets the group to 5 which specifies 1536-bit base prime numbers.
```
group 5
hash

Configures the IKE hash protocol to use during IKE SA negotiations.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

hash { md5 | sha1 }
[ default | no ] hash

default
Restores the default setting of this parameter.

no
Removes a previously configured hash algorithm.

md5
Specifies that the hash protocol is Message Digest 5 truncated to 96 bits.

sha1
Specifies that the hash protocol is Secure Hash Algorithm-1 truncated to 96 bits. This is the default setting for this command.

Usage
Use this command to configure the hash algorithm used during key negotiation.

Example
Set the hash algorithm to Message-Digest 5 by entering the following command:
hash md5
**lifetime**

Configures the lifetime of the IKE Security Association (SA).

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
lifetime seconds

default lifetime
```

- `default`
  Restores the default setting of this parameter.

- `seconds`
  Default: 86400
  The number of seconds for the SA to live. `seconds` must be an integer from 60 to 86400.

**Usage**

Use this command to set the time that an ISAKMP SA will be valid. The lifetime is negotiated with the peer and the lowest configured lifetime duration is used.

**Example**

The following command sets the SA lifetime to 100 seconds:

```
lifetime 100
```
Chapter 138
IP VRF Context Configuration Mode Commands

The IP Virtual Routing and Forwarding Context Configuration Mode is used to create and manage the VRF context instance for GRE tunneling interfaces for addresses, address resolution options, etc.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          Ip vrf vrf_name
            IP VRF Context Configuration Mode
```

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

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`end`

**Usage**

Change the mode back to the Exec mode.
**exit**

Exits the Interface Configuration Mode and returns to the Context Configuration Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```sh
exit
```

**Usage**

Return to the context configuration mode.
ip maximum-routes

This command configures the maximum number of routes in an IP VRF routing table configured in this context.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ip maximum-routes max_routes
no ip maximum-routes

max_routes
Sets the maximum number of routes in a specific IP VRF context.
max_routes must be an integer between 1 through 16384 on ASR 5000 system.

Usage
Use this command to configure the maximum number of routes in a particular VRF routing table. When the number of routes in the VRF is more than the maximum limit configured, a critical log is generated indicating that the number of routes is over the limit. Once the number of routes in the VRF goes under the limit, a clear log is generated.

The maximum routes configured using this command will be sent to the threshold configuration logic for appropriate action. For more information on threshold configuration, refer threshold route-service bgp-routes and threshold poll route-service interval commands in Global configuration mode.

Example
The following command sets 1000 routes as a maximum limit for specific VRF context:

   ip maximum-routes 1000
**mpls map-dscp-to-exp**

This command provides mapping of final differentiated services code point (DSCP) bit value in IP packet header to final Experimental (EXP) bit value in MPLS header for incoming traffic.

### Product
All

### Privilege
Security Administrator, Administrator

### Syntax
```
mpls map-dscp-to-exp dscp dscp_bit_value exp exp_bit_value
```

**dscp dscp_bit_value**
This keyword specifies the final DSCP bit value which is to map with the final EXP bit value in MPLS header for incoming traffic.

*dscp_bit_value* specifies the value of DSCP bit values separated in 8 groups and represented with integers between 0 through 7.

The default representation of DSCP value in 8 groups is given in the following table:

<table>
<thead>
<tr>
<th>DSCP Marking Value</th>
<th>DSCP Map Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>0</td>
</tr>
<tr>
<td>8-15</td>
<td>1</td>
</tr>
<tr>
<td>16-23</td>
<td>2</td>
</tr>
<tr>
<td>24-31</td>
<td>3</td>
</tr>
<tr>
<td>32-39</td>
<td>4</td>
</tr>
<tr>
<td>40-47</td>
<td>5</td>
</tr>
<tr>
<td>48-55</td>
<td>6</td>
</tr>
<tr>
<td>56-63</td>
<td>7</td>
</tr>
</tbody>
</table>

**exp exp_bit_value**
This keyword specifies the final EXP bit value in MPLS header to which the final DSCP bit value 0 to 7 (represented in 8 values) coming from incoming traffic will be mapped.

*exp_bit_value* is the value of EXP bit in MPLS header and must be an integer between 0 through 7.

### Usage
Use this command to map the final DSCP value coming from incoming IP traffic to a final EXP value in MPLS header. This mapping determines the QoS and service parameters to which the packet is assigned.

### Example
The following command maps the DSCP value 3 (24 to 31) to EXP bit 3 in MPLS header:

```
mpls map-dscp-to-exp dscp 3 exp 3
```
**mpls map-exp-to-dscp**

This command provides mapping of incoming Experimental (EXP) bit value in MPLS header to internal differentiated services code point (DSCP) bit value in IP packet header for outgoing traffic.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
mpls map-exp-to-dscp exp exp_bit_value dscp dscp_bit_value
```

- **exp exp_bit_value**
  This keyword specifies the incoming EXP bit value in MPLS header to which the internal DSCP bit value 0 to 7 (represented in 8 values) in IP traffic will be mapped.
  `exp_bit_value` is the value of EXP bit in MPLS header and must be an integer between 0 through 7.

- **dscp dscp_bit_value**
  This keyword specifies the DSCP bit value is to be mapped with the incoming EXP bit value in MPLS header.
  `dscp_bit_value` specifies the value of DSCP bit values separated in 8 groups and represented with integers between 0 through 7.

The default representation of DSCP value in 8 groups is given in the following table:

<table>
<thead>
<tr>
<th>DSCP Marking Value</th>
<th>DSCP Map Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>0</td>
</tr>
<tr>
<td>8-15</td>
<td>1</td>
</tr>
<tr>
<td>16-23</td>
<td>2</td>
</tr>
<tr>
<td>24-31</td>
<td>3</td>
</tr>
<tr>
<td>32-39</td>
<td>4</td>
</tr>
<tr>
<td>40-47</td>
<td>5</td>
</tr>
<tr>
<td>48-55</td>
<td>6</td>
</tr>
<tr>
<td>56-63</td>
<td>7</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to map the incoming EXP bit value in MPLS header to DSCP bit value in IP traffic. This mapping determines the QoS and service parameters to which the packet is assigned.

**Example**
The following command maps the EXP bit value 4 to DSCP value 6 (48 to 55) in IP header:

```
mpls map-exp-to-dscp exp 4 dscp 6
```
Chapter 139
IuPS Service Configuration Mode Commands

The IuPS Service configuration mode is used to define properties for the IuPS service which controls the Iu-PS interface connections to Radio Network Controllers (RNCs) of the UMTS Terrestrial Radio Access Network (UTRAN).

```
IuPS Service Configuration Mode
  iups-service name
    context name
      configure
        Global Configuration Mode
          context name
            Exec Mode
```

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

This command configures the access protocol parameters for the IuPS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

access-protocol sccp-network sccp_net_id
no access-protocol sccp-network sccp_net_id

no
Removes a previously configured access protocol value.

sccp-network sccp_net_id
Specifies the Signaling Connection Control Part (SCCP) for this IuPS service to use. sccp_net_id must be an integer from 1 to 16.

Usage
Use this command to configure access protocol parameters for the current IuPS service.

Example
The following command specifies that the current Iu-PS service should use SCCP 1:

access-protocol sccp-network 1
blacklist-timeout-gtpu-bind-addresses

This command specifies the time period that a GTP-U bind address (loopback address) will not be used (is blacklisted) in RAB-Appliance requests after a RAB assignment request, with that GTP-U bind address, has been rejected by an RNC with the cause - Unspecified Error. This is a failure at the RNC’s GTP-U IP interface.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

blacklist-timeout-gtpu-bind-addresses seconds

default blacklist-timeout-gtpu-bind-addresses

default
Resets the blacklist time to 60 seconds.

seconds
Number of seconds that the GTP-U bind (loopback) address will not be used in a RAB-Appliance request. seconds: Must be an integer from 1 to 1800.

Usage
Use this command to configure the blacklist period.

Example
The following command specifies a 15 minutes blacklist period.

blacklist-timeout-gtpu-bind-addresses seconds 460
**end**

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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```plaintext
d exit
```

**Usage**
Return to the Exec mode.
**exit**

Exits the current configuration mode and returns to the previous configuration mode, the context configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the context configuration mode.
**gtpu**

This command configures parameters for the GTP user (GTP-U) dataplane.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gtpu { bind ip_addr | echo-interval seconds | max-retransmissions number | retransmission-timeout seconds }

no gtpu { bind address ip_addr | echo-interval | max-retransmissions | retransmission-timeout }

default gtpu { echo-interval | max-retransmissions | retransmission-timeout }
```

- **no**
  Removes the configured parameter value.

- **default**
  Sets the specified parameter to its default setting.

- **bind address ip_addr**
  This command binds the specified IP address to the Iu-PS GTP-U endpoint.
  `ip_addr`: Must be an IP v4 IP address in dotted decimal notation.

- **echo-interval seconds**
  Default: 60
  Configures the rate, in seconds, at which GTP-U echo packets are sent to the UTRAN over the Iu-PS interface.
  `seconds`: Must be an integer from 60 through 3600.

- **max-retransmissions number**
  Default: 5
  Configures the maximum number of transmission retries for GTP-U packets.
  `number`: Must be an integer from 0 through 15.

- **retransmission-timeout seconds**
  Default: 5
  Configures the retransmission timeout for GTP-U packets in seconds.
  `seconds`: Must be an integer from 1 through 20.

**Usage**
Use this command to configure GTP-U parameters for the Iu-PS interface.

**Example**
The following command binds the IP address 192.168.0.10 to the Iu-PS interface for communication with the UTRAN:

```
gtpu bind address 192.168.0.10
```
iu-hold-connection

Defines the type and duration of the Iu hold connection.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

    iu-hold-connection { always [ hold-time time ] | requested-by-ms [ hold-time time ] }
    [ default | no ] iu-hold-connection

default
Resets the Iu hold connection parameters to requested-by-ms and 100 second duration.

no
Removes the configuration information for the specified Iu hold connection parameter.

always
Specifies that there is always to be an Iu hold connection procedure.

requested-by-ms
Specifies that there is only an Iu hold connection procedure if requested by the MS/UE. This is the default setting for Iu-hold-connection.

hold-time time
This variable configures the interval (in seconds) that the SGSN holds the Iu connection. time: must be an integer from 10 to 3600. Default is 100.

Usage
Define the amount of time the Iu connection will be held open.

Example

    iu-hold-connection always hold-time 120
**iu-recovery**

This command enables the Iu recovery function.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
iu-recovery

no iu-recovery
```

**Usage**
Enable or disable Iu recovery function that should be used whenever sessions are recovered.

**Example**
The following command disables the Iu Recovery function:
```
no iu-recovery
```
iu-release-complete-timeout

Configures the SGSN’s timer for waiting for an Iu Release Complete message from the RNC.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
  iu-release-complete-timeout time

  default iu-release-complete-timeout
```

- **default**
  Resets the timer to its default setting.

- **time**
  This variable defines the amount of time (in seconds) that the SGSN waits to receive an ‘Iu Release Complete’ message from the RNC.
  Default: 10.
  `time`: Must be an integer from 1 to 60.

**Usage**
Configure the number of seconds that the SGSN waits to receive the Iu Release Complete message.

**Example**

```
iu-release-complete-timeout 20
```
loss-of-radio-coverage ranap-cause

This command sets the detection cause included in the Iu Release message. This command is unique to releases 9.0 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```yaml
loss-or-radio-coverage ranap-cause cause_number

default loss-of-radio-coverage ranap-cause
```

**default**
This keyword resets the configuration to the default cause ID number.

**ranap-cause cause_number**
This number identifies the reason the SGSN has detected, from Iu Release messages, for the loss of radio coverage (LORC). This value is included in the IE messages the SGSN sends to either the GGSN or the GGSN and the peer SGSN to indicate LORC state. The range of reasons is a part of the set defined by 3GPP 25413.

`cause_number`: Must be an integer from 1 to 512.
Default: 46 (MS/UE radio connection lost)

**Usage**
By defining a cause code, the SGSN knows to detect the LORC state of the mobile from Iu Release messages it receives for the subscriber. This configuration also instructs the SGSN to include the defined cause code for the LORC state in the IE portion of various messages sent to the GGSN and optionally the peer SGSN. This command is one of the two commands required to enable the SGSN to work with the GGSN and, optionally the peer SGSN, to implement the Overcharging Protection feature (see the SGSN Overview in the SGSN Administration Guide for feature details. The other command needed to implement the Overcharging Protection feature is the gtp private extension command explained in the SGSN APN Policy Configuration Mode chapter of the Command Line Interface Reference.

**Example**
Use the following command to set the cause code to indicate that there are no radio resources available in the target cell, cause 53.

```yaml
loss-or-radio-coverage ranap-cause 53
```
plmn

Configures the PLMN (public land mobile network) related parameters for the IuPS service. This command is applicable to releases 8.1 and higher.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax


no plmn id

no
Removes the PLMN ID from the configuration.

mcc mnc_num
Specifies the mobile country code (MCC) portion of the PLMN’s identifier. mcc_num is the PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc mnc_num
Specifies the mobile network code (MNC) portion of the PLMN’s identifier. mnc_num is the PLMN MNC identifier and can be configured to any 2 or 3 digit value between 00 and 999.

network-sharing common-plmn mcc mnc_num mnc mnc_num
When network sharing is employed, this set of keywords is required to define the PLMN ID of the common PLMN. The common PLMN is usually different from a local PLMN.

plmn-list mcc mnc_num mnc mnc_num
When network sharing is employed and more than two PLMNs are available, then use the plmn-list keyword to begin a list of all additional PLMNs.

Usage

Use this command to configure the PLMN associated with the SGSN. There can only be one PLMN associated with an SGSN unless one of the following features is enabled and configured: network sharing or multiple PLMN.

For network sharing, use the network-sharing keywords to identify more than one PLMN. Including the PLMN identified initially. None have precedence. They are all treated equally but they must each be unique. In a MOCN configuration, the PLMN list will not be used as there would only be one local PLMN.

For multiple PLMN support, the SGSN can support up to 8 Iu-PS configurations for PLMNs. These Iu-PS service configurations must be associated with the SGSN via the ran-protocol command in the SGSN Service configuration mode.
Example
Use the following command to identify a PLMN and instruct the SGSN to perform network sharing with a single PLMN:

```
plmn id mcc 313 mnc 23 network-sharing common-plmn mcc 404 mnc 123
```
rab-assignment-response-timeout

Configures the RAB assignment timer.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
rab-assignment-response-timeout time

default rab-assignment-response-timeout
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Resets the timer to its default setting.</td>
</tr>
<tr>
<td><code>time</code></td>
<td>This variable configures the amount of time (in seconds) that the SGSN waits to receive a RAB assignment from the RNC.</td>
</tr>
</tbody>
</table>

`time`: must be an integer from 1 to 60.  
Default: 8.

**Usage**

This command defines time the SGSN waits for the completion of the RAB assignment procedure.

**Example**

Change the timer setting to 11 seconds.

```
rab-assignment-response-timeout
```
radio-network-controller

This command creates an instance of an RNC configuration to associate with the IuPS service for the SGSN. This command is only available in release 8.0; use the rnc command for releases 8.1 and higher.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

radio-network-controller id rnc_id mcc mcc_num mnc mnc_num
no radio-network-controller id rnc_id mcc mcc_num mnc mnc_num

no
Removes the configuration information for the specified RNC.

id rnc_id
Define the instance number of the RNC configuration.
  rnc_id: Must be an integer from 0 to 4095.

mcc mcc_num
Specifies the mobile country code (MCC).
  mcc_num: Must be an integer between 100 and 999.

mnc mnc_num
Specifies the mobile network code (MNC).
  mnc_num: Must be an integer between 00 and 999.

Usage
Use this command to configure information for the IuPS service to use to contact specific RNCs. This command also provides access to the RNC configuration mode.

Example
The following command creates or accesses an instance of an RNC configuration.

  radio-network-controller id 1 mcc 131 mnc 22
relocation-complete-timeout

This command specifies the maximum time for the SGSN to wait for a Relocation Completion from the core network.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
relocation-complete-timeout timeout_value
default relocation-complete-timeout
```

- **default**
  resets the configuration to a 5 second wait time.

- **timeout_value**
  time in seconds that the SGSN waits for relocation to be completed.
  `timeout_value`: Must be an integer from 1 to 60.
  Default: 5 seconds.

**Usage**

Use this command to configure the number of seconds the SGSN will wait for a relocation to be completed. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

**Example**

The following command sets the wait time for 10 seconds.

```
relocation-complete-timeout 10
```
reset

Defines the configuration specific to the RESET procedure.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
reset { ack-timeout time | guard-timeout time | max-retransmissions retries |
          sgsn-initiated }
```

```
default reset { ack-timeout | guard-timeout | max-retransmissions | sgsn-initiated }
```

```
no reset sgsn-initiated
```

---

**default**

Returns to the default settings for the Reset procedure.

---

**no**

Removes the SGSN-initiated reset procedure from the configuration.

---

**ack-timeout time**

Configures the interval (in seconds) for which the SGSN waits for RESET-ACK from the RNC.

`time` must be an integer from 5 to 10.

Default: 10.

---

**guard-timeout**

Configures the interval (in seconds) after which the SGSN sends RESET-ACK to the RNC.

`time` must be an integer from 5 to 10.

Default: 10

---

**max-retransmissions**

Configures the maximum retries for RESET message.

`retries` must be an integer from 1 to 2.

Default: 1.

---

**sgsn-initiated**

Enables SGSN initiated RESET procedure.

Default: disabled.

---

**Usage**

Configures the parameters that determine a RESET.
Example
Use the following to have the SGSN initiate the RESET procedure:

   reset sgsn-initiated
rnc

This command creates or accesses an instance of an RNC (radio network controller) configuration.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

rnc id rnc_id

nornc id rnc_id

   no
   Removes the configuration information for the specified RNC.

   idrnc_id
   Set the identification number of the RNC configuration instance.
   rnc_id: Must be an integer from 0 to 4095 for 8.1 releases. Must be an integer from 0 to 65535 for releases 9.0 and higher.

Usage
Use this command to configure information for the IuPS service to use to contact specific RNCs. This command also provides access to the RNC configuration mode.

Example
The following command creates an RNC configuration instance

   rnc id 1
security-mode-complete-timeout

This command configures the security mode timer.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
security-mode-complete-timeout time

default security-mode-complete-timeout
```

**default**

Resets the timer configuration to the default settings.

**time**

Configures the interval (in seconds) the SGSN waits for the security mode from the MS to complete.

- `time` must be an integer from 1 to 60.
- Default is 5

**Usage**

Use this command to configure the timer that determines how long the SGSN waits for a Security Mode Complete message from the MS (mobile station).

**Example**

```plaintext
security-mode-complete-timeout 7
```
srns-context-response-timeout

This command configures the SGSN context response timer.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
srns-context-response-timeout time
```

```
default srns-context-response-timeout
```

```
default
Resets the timer configuration to the default setting.
```

```
time
Configures the interval (in seconds) for which the SGSN waits for an SRNS Context Request message. 
 time must be an integer from 1 to 60. 
 Default: 5.
```

Usage
Configures the time to wait before the SGSN sends a response to the SRNS ‘context request’ message.

Example
```
srns-context-response-timeout 7
```
tigoc-timeout

This command configures the TigOc interval.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

tigoc-timeout time

default tigoc-timeout

default
Resets the timer configuration to the default setting.

time
This command sets the time in seconds.
time: Must be an integer from 1 to 10.
Default: 5.

Usage
Define the amount of time that the SGSN ignores any overload messages for TigOc interval after receiving one overload message from the RNC.

Example
Use the following command to change the default TigOc interval:

tigoc-timeout 4
tintc-timeout

This command configures the TinTc interval.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
tintc-timeout time
```

default tintc-timeout

default
Resets the timer configuration to the default setting.

time
Set the number of seconds to wait. 
time: Must be an integer from 1 to 10.
Default: 5.

Usage
Define the number of seconds that the SGSN waits before decrementing (by one) the traffic level of the RNC.

Example

```
tintc-timeout 4
```
Chapter 140
LAC Service Configuration Mode Commands

The LAC Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Access Concentrator (LAC) services facilitate tunneling to peer L2TP Network Servers (LNSs).

```
Exec Mode
   configure
      Global Configuration Mode
         context name
            Context Configuration Mode
               lac-service name
                  LAC Service Configuration Mode
```

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

This command configure the system to allow different attributes in the LAC Hostname AVP and Called-Number AVP for L2TP messages exchanged between LAC and LNS.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
allow {aaa-assigned-hostname | called-number value apn}
[ no | default ] allow {aaa-assigned-hostname | called-number value apn}
```

**no**
Disable the configured attribute and returns to the behavior that uses the LAC-Service name as the HostName AVP.

**aaa-assigned-hostname**
When enabled if AAA assigns a valid Tunnel-Client-Auth-ID attribute for the tunnel, it is used as the HostName AVP in the L2TP tunnel setup message.
This keyword works in conjunction with `local-hostname hostname` keyword applied with `tunnel l2tp` command in APN configuration mode.
When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in APN are considered for the LNS peer selection. When APN configuration is selected, local-hostname configured with `tunnel l2tp` command in the APN for the LNS peer will be used as a LAC Hostname.

**called-number value apn**
This keyword configures the system to send APN name in Called-Number AVP as a part of ICRQ message sent to the LNS. If this keyword is not configured, Called-Number AVP will not be included in ICRQ message sent to the LNS.

**Usage**

Use this command to configure the attribute for the HostName AVP for L2TP messages exchanged between LAC and LNS.
LAC Hostname will be different for the subscribers corresponding to the different corporate APNs. In the absence of a AAA assigned HostName, the LAC-Service name is used as HostName. By default the LAC-Service name is used as the HostName AVP.

**Example**
The following command enables the use of the value of Tunnel-Client-Auth-ID attribute for the HostName AVP:

```
allow aaa-assigned-hostname
```
Use the following command to reset the behavior so that the LAC-Service uses the LAC-Service name as the HostName AVP:

```plaintext
no allow aaa-assigned-hostname
```
bind

This command assigns a local end point address to the LAC service in the current context.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax
bind ip_address [max-subscribers]
no bind ip_address

Usage
Use this command to bind a local end point IP address to the LAC service.

Example
The following command binds the local end point IP address 10.10.10.100 to the LAC service in the current context:

\[\text{bind 10.10.10.100}\]

The following command removes the binding of the local end point to the LAC service:

\[\text{no bind}\]
data sequence-number

Enables data sequence numbering for sessions that use the current LAC service. Data sequence numbering is enabled by default.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
data sequence-number
no data sequence-number
```

```
no
```

Disables data sequence numbering for sessions.

Usage
An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

Example
Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```
default

This command sets the specified LAC service parameter to its default value or setting.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
default {data sequence-number | hide-attributes | keepalive-interval | load-balancing | local-receive-window | max-retransmission | max-session-per-tunnel | max-tunnel-challenge-length | max-tunnels | proxy-lcp-authentication | retransmission-timeout-first | retransmission-timeout-max | trap all | tunnel-authentication}
```

data sequence-number
Enables data sequence numbering for sessions.

hide-attributes
Disables hiding attributes in control messages sent from the LAC to the LNS.

keepalive-interval
Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 secs.

load-balancing
Sets the load balancing algorithm to be used when many LNS peers have been configured to the default of round robin.

local-receive-window
Sets the window size to be used for the local side for the reliable control transport to the default of 16.

max-retransmission
Sets the maximum number of retransmissions to the default of 5.

max-session-per-tunnel
Sets the maximum number of sessions per tunnel at any point in time to the default of 512.

max-tunnel-challenge-length
Sets the maximum length of the tunnel challenge to the default of 16 bytes.

max-tunnels
Sets the maximum number of tunnels for this service to the default of 32000.
proxy-lcp-authentication
Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first
Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max
Sets the maximum retransmit interval to the default of 8 seconds.

trap all
Generates all supported SNMP traps.

tunnel-authentication
Sets tunnel authentication to the default state of enabled.

Usage
Use the default command to set LAC service parameters to their default states.

Example
Use the following command to set the keep alive interval to the default value of 60 seconds:
default keepalive-interval
Use the following command to set the maximum number of sessions per tunnel to the default value of 512:
default max-session-per-tunnel
**hide-attributes**

Enables hiding certain attributes (such as proxy-auth-name and proxy-auth-rsp) in control messages sent from the LAC to the LNS. The LAC hides such attributes only if tunnel authentication is enabled between the LAC and the LNS.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
hide-attributes
no hide-attributes
```

**Usage**
Use this command to hide certain attributes from control messages when tunnel authentication is enabled between the LAC and the LNS.

**Example**
The following command enables hiding attributes:
```
hide-attributes
```
keepalive-interval

This command specifies the amount of time to wait before sending a Hello keep alive message.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
keepalive-interval seconds
no keepalive-interval
```

- **no**
  Disables the generation of Hello keep alive messages on the tunnel.

- **seconds**
  Default: 60
  The number of seconds to wait before sending a Hello keep alive message. The number can be configured to any integer value from 30 to 2147483648.

Usage

Use this command to set the amount of time to wait before sending a Hello keep alive message or disable the generation of Hello keep alive messages completely. A keep alive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example

Use the following command to set the Hello keep alive message interval to 120 seconds:
```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keep alive messages:
```
no keepalive-interval
```
### load-balancing

Configures how LNSs are selected for this LAC service.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
load-balancing {balanced | prioritized | random}
```

**balanced**

LNS selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of LNS nodes available.

**prioritized**

LNS selection is made based on the priority assigned in the Tunnel-Preference attribute. An example of this method is three LNS nodes, with preferences of 1, 2, and 3 respectively. In this example, the RADIUS server always tries the tunnel with a preference of 1 before using any of the other LNS nodes.

**random**

Default: Enabled

LNS selection is random in order, wherein the RADIUS server does not use the Tunnel-Preference attribute in determining which LNS to select.

**Usage**

Use this command to configure the load-balancing algorithm that defines how the LNS node is selected by the LAC when there are multiple peer LNSs configured in the LAC service.

**Example**

The following command sets the LAC service to connect to LNSs in a sequential order;

```
load-balancing balanced
```

The following command sets the LAC service to connect to LNSs according to the priority assigned through the Tunnel-Preference attribute:

```
load-balancing prioritized
```
**local-receive-window**

Specifies the number of control messages the remote peer LNS can send before waiting for an acknowledgement.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
local-receive-window integer
```

*integer*

Default: 4

The number of control messages to send before waiting for an acknowledgement. The number can be configured to any integer value from 1 to 256.

**Usage**

Use this command to set the size of the control message receive window being offered to the remote peer LNS. The remote peer LNS may send the specified number of control messages before it must wait for an acknowledgement.

**Example**
The following command sets the local receive window to 10 control messages:

```
local-receive-window 10
```
max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
max-retransmission integer
```

- `integer`
- Default: 5
- The maximum number of retransmissions of a control message to a peer. This value must be an integer in the range of 1 to 10.

**Usage**

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.

Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within it.

**Example**

The following command sets the maximum number of retransmissions of a control message to a peer to 7:

```
max-retransmissions 7
```
max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single a tunnel at any time.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

max-sessions-per-tunnel integer

integer
Default: 512
The maximum number of sessions. This value must be in the range of 1 to 65535.

Usage
Use this command to set the maximum number of sessions you want to allow in a tunnel.

Example
The following command sets the maximum number of sessions in a tunnel to 5000:
max-sessions-per-tunnel 5000
max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes. The challenge is used for tunnel authentication purposes during tunnel creation.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
max-tunnel-challenge-length bytes
```

`bytes`

Default: 16
The number of bytes to set the maximum length of the tunnel challenge. This must be a value from 4 to 32.

Usage
Use this command to set the maximum length, in bytes, for the tunnel challenge that is used during tunnel creation.

Example
The following command sets the maximum length of the tunnel challenge to 32 bytes:
```
max-tunnel-challenge-length 32
```
max-tunnels

The maximum number of tunnels that the current LAC service can support.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
max-tunnels integer
```

**Usage**

Use this command to set the maximum number tunnels that this LAC service can support at any on time.

**Example**

Use the following command to set the maximum number of tunnels for the current LAC service to 20000:

```
max-tunnels 20000
```
peer-lns

Adds a peer LNS address for the current LAC service. Up to 8 peer LNSs can be configured for each LAC service.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax
peer-lns ip_address [encrypted] secret secret [crypto-map map_name { [encrypted] isakmp-secret secret }] [description text] [ preference integer ]
no peer-lns ip_address

no peer-lns ip_address
Deletes the peer LNS at the IP address specified by ip_address. ip_address must be entered in standard IPv4 dotted decimal notation.

ip_address
The IP address of the peer LNS for the current LAC service. ip_address must be entered in standard IPv4 dotted decimal notation.

[encrypted] secret secret
Designates the secret which is shared between the current LAC service and the peer LNS. secret must be a string from 1 to 256 alpha and/or numeric characters and is case sensitive.

encrypted secret secret: Specifies that encryption should be used when communicating the secret with the peer LNS.

crypto-map map_name { [encrypted] isakmp-secret secret }
map_name is the name of a crypto map that has been configured in the current context. map_name must be a string from 1 to 127 alpha and/or numeric characters and is case sensitive.

isakmp-secret secret: The pre-shared key for IKE. secret must be a string from 1 to 127 alpha and/or numeric characters and is case sensitive.

encrypted isakmp-secret secret: The pre-shared key for IKE. Encryption must be used when sending the key. secret must be a string from 1 to 127 alpha and/or numeric characters.

description text
Specifies the descriptive text to use to describe the specified peer LNS. text must be 0 to 79 alpha and/or numeric characters with no spaces or a quoted string of printable characters.

preference integer
This sets the priority of the peer LNS if multiple peer LNSs are configured. integer must be a value ranging from 1 to 128.

Usage
Use this command to add a peer LNS address for the current LAC service.
**Example**
The following command adds a peer LNS to the current LAC service with the IP address of 10.10.10.100, sets encryption on, specifies the shared secret to be 1b34nnf5d and sets the preference to 3:
peer-lns 10.10.10.100 encrypted secret 1b34nnf5d preference 3
The following command removes the peer LNS with the IP address of 10.10.10.200 for the current LAC service:
no peer-lns 10.10.10.200
proxy-lcp-authentication

Enables and disables the sending of proxy LCP authentication parameters to the LNS.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
proxy-lcp-authentication
no proxy-lcp-authentication

no
Disables the sending of proxy LCP authentication parameters to the LNS.

proxy-lcp-authentication
Default: Enabled
Enables the sending of proxy LCP authentication parameters to the LNS.
```

**Usage**

Use this feature in situations where the peer LNS does not understand the proxy LCP Auth AVPs that the system sends and does not do an LCP renegotiation and tears down the call.

**Example**

Use the following command to disable the sending of proxy LCP authentication parameters to the LNS;
```
no proxy-lcp-authentication
```
Use the following command to re-enable the sending of proxy LCP authentication parameters to the LNS
```
proxy-lcp-authentication
```
retransmission-timeout-first

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. This command sets the initial timeout for retransmission of control messages.

Privilege
Security Administrator, Administrator

Syntax
```
retransmission-timeout-first integer
```

integer
Default: 1
The amount of time to wait before sending the first control message retransmission. This value is measured in seconds and must be an integer from 1 to 100.

Usage
Use this command to set the initial timeout before retransmitting control messages to the peer.

Example
The following command sets the initial retransmission timeout to 3 seconds:
```
retransmission-timeout-first 3
```
retransmission-timeout-max

This command configures maximum amount of time between two retransmission of control messages.

Privilege
Security Administrator, Administrator

Syntax
```plaintext
retransmission-timeout-max integer
```

integer

Default: 8

integer is the maximum time in seconds to wait before retransmitting control messages and must be an integer between 1 through 100.

Usage
Use this command to set the maximum amount of time that can elapse before retransmitting control messages.

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval.

Example
The following command sets the maximum retransmission time-out to 10 seconds:
```plaintext
retransmission-timeout-max 10
```
single-port-mode

This command enables/disables the L2TP LAC service always to use standard L2TP port 1701 as source port for all L2TP control and data packets originated from LAC node.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no | default] single-port-mode
```

- **no**
  
  Disables the configured single source port configuration from this LAC service.

- **default**
  
  Default: Enabled
  
  Sets this command to default state of disabled. By default single source port configuration for L2TP LAC packets is disabled.

**Usage**

Use this command to enable or disable the single port mode for L2TP LAC service.

If this feature is enabled, then L2TP LAC service will always use standard L2TP port 1701 as source port for all L2TP control/data packets originated from LAC (instead of the default scheme in which each L2TPMgr uses a dynamic source port). L2TPMgr instance 1 will handle all L2TP calls for the service.

**Caution:** Changing this configuration, while the service is already running, will cause restart of the service.

**Example**

The following command enables the LAC service to use port 1701 as source port for all L2TP control and data packets:

```
single-port-mode
```
snoop framed-ip-address

When enabled, this feature allows the LAC to detect IPCP packets exchanged between the mobile node and the LNS and extract the framed-ip-address assigned to the mobile node. The address will be reported in accounting start/stop messages and will be displayed for subscriber sessions.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax
snoop framed-ip-address
no snoop framed-ip-address
default snoop framed-ip-address

no
Disables the feature. Accounting start/stop will occur before the PPP session is established and the framed IP address field will be reported as 0.0.0.0.

default
Disabled.

Usage
This feature is available to address simple IP roaming scenarios. If this feature is enabled, the accounting start will be sent only after the framed-ip-address is detected. If the framed-ip-address is not detected within 16 seconds, an accounting start will be sent for the session with the 0.0.0.0 address. If the session is disconnected during the detection attempt, accounting start/stop will be sent for the session. If the session renegotiates IPCP, an accounting stop will be generated with a framed-ip-address from the old session and an accounting start will be generated with an IP address for the new session. IPv6 address detection is not supported.

Important: When this feature is enabled and the show subscribers all command is invoked, the framed-IP-address is displayed for the PDSN Simple IP subscriber in the output display.
trap

This command generates SNMP traps.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```plaintext
trap all
no trap all
```

Disables SNMP traps.

Usage
Use this command to enable/disable all supported SNMP traps.

Example
To enable all supported SNMP traps, enter the following command:
```
trap all
```
tunnel-authentication

Enables tunnel authentication. When tunnel authentication is enabled, a configured shared secret is used to ensure that the LAC service is communicating with an authorized peer LNS. The shared secret is configured by the `r_peer-lns` command in the LAC service configuration mode, the `R_tunnel 12tp` command in the subscriber configuration mode, or the `Tunnel-Password` attribute in the subscribers RADIUS profile.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
tunnel-authentication
no tunnel-authentication

no
```

Disables tunnel authentication
Tunnel authentication is enabled by default.

Usage
Disable or enable the usage of secrets to authenticate a peer LNS when setting up a tunnel.

Example
To disable tunnel authentication, use the following command:
`no tunnel-authentication`
To re-enable tunnel authentication, use the following command:
`tunnel-authentication`
tunnel selection-key

This command enables the support to create tunnels between L2TP service and an LNS server on the basis of value of attribute “Tunnel-Server-Auth-ID” received from AAA server.

Privilege
Security Administrator, Administrator

Syntax
```
tunnel selection-key { tunnel-server-auth-id | none } 
[default] tunnel selection-key
```

**default**
This keyword disables the creation of tunnel between LAC service and LNS based on key value received in attribute, “Tunnel-Server-Auth-ID” from AAA server.

**tunnel-server-auth-id**
Default: Enabled
This keyword enables the creation of tunnels between LAC service on GGSN and an LNS server on the basis of domain attribute, “Tunnel-Server-Auth-ID”, value received from AAA server.

**none**
Default: Enabled
This keyword disables the creation of multiple tunnels between a pair of LAC service on GGSN and LNS server. LAC will not make use of key to choose a tunnel with LNS in this setup.

**Usage**
Use this command to enable or disable the creation of additional L2TP tunnels between LAC service on GGSN and LNS server on the basis of “Tunnel-Server-Auth-ID” attribute value received from AAA Server in Access-Accept message. This value of attribute is treated as a key for tunnel selection and creation.

When the LAC needs to establish a new L2TP session, it would first check if there is already an existing L2TP tunnel with the peer LNS based on the value of key configured. If no such tunnel exists for the key, it will create a new Tunnel with the LNS.

Default configuration have selection-key as **none**. Hence, LAC will not make use of key to choose a tunnel with LNS, in default setup.

Maximum number of session as configured with **max-sessions-per-tunnel** command will be applicable for each tunnel created through this command. By default each tunnel supports 512 sessions.

If LAC service needs to establish a new tunnel for new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message for the APN/subscriber. If all available peer-LNS are exhausted, LAC service will reject the call.

**Example**
The following command enables the use of “Tunnel-Server-Auth-ID” attribute value received from AAA Server in Access-Accept message as a key for tunnel selection and creation:
```
tunnel selection-key tunnel-server-auth-id
```
Chapter 141
Line Configuration Mode Commands

The Line Configuration Mode is used to manage the terminal line characteristics for output formatting.

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

Restores the default length or width for the output to the display terminal.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default { length | width }
```

<table>
<thead>
<tr>
<th>length</th>
<th>width</th>
</tr>
</thead>
</table>

**Usage**

Reset the output display properties if they had been changed during a session.

**Example**

```
default length
default width
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the line configuration mode and returns to the global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the global configuration mode.
length

Configures the output for the displays length (number of rows).

Privilege
Security Administrator, Administrator

Syntax
length number

number

Specifies the number of rows (lines) of output that can be displayed at one time for the display (output) terminal. number must have a value of 0 or be in the range from 5 through 512 where the special value 0 implies an infinite number of rows.

Usage
Set the current session’s display terminal has different display characteristics than the defaults. The special infinite value (0) is typically used when logging the output of a session from a remote machine since this will result in no pagination of output.

Example
The following commands set the length of the display to infinite and 33, respectively.

length 0
length 33
**width**

Configures the output for the displays width (number of columns/characters wide).

**Privilege**

Security Administrator, Administrator

**Syntax**

```
width number
```

Specifies the number of columns (characters) of output that can be displayed at one time for the display (output) terminal. `number` must have a value in the range from 5 through 512.

**Usage**

Set the current session’s display terminal has different display characteristics than the defaults.

**Example**

```
width 160
```
Chapter 142
Link Configuration Mode Commands

The Link configuration mode defines the MTP3 link parameters for a specific link in a linkset of an SS7 routing domain instance.

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

This command configures link arbitration.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
arbitration { active | passive }
no arbitration
```

**Active**

The SSCOP initiates the transmission of PDUs.

**Passive**

The SSCOP waits to receive PDUs.

**Usage**

Sets the configuration to initiate transmission of PDUs.

**Example**

```
arbitration active
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
exit
```

**Usage**

Returns to the previous mode.
**mtp2-lssu-len**

This command sets the length of the link status signal unit (LSSU) which carries link status information used to manage link alignment and indicate the status of the signaling points to each other.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mtp2-lssu-len #_octets
default mtp2-lssu-len
```

- **default**

  Using this keyword with the command resets the length to the default of 1 octet.

- **#_octets**

  Sets the number of octets for the length of the LSSU.

  `#_octets`: Must be either 1 or 2.

**Usage**

Use this command to define the maximum amount of link status information that is to be shared between signaling points.

**Examples**

Set the LSSU length to 2 octets - the maximum length.

```
mtp2-lssu-len 2
```
**lmtp3-discard-priority**

Configure MTP3 message discard priority.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mtTp3-discard-priority priority
default mtTp3-discard-priority
```

- **default**
  Resets the priority to the default value.

- **priority**
  `priority`: must be an integer between 0 and 3. Default is 0.

**Usage**

Use this command to manage MTP3 messaging.

**Example**

```
mtTp3-discard-priority 2
```
**mtp3-max-slt-try**

Configure maximum number of times to retry SLT (signaling link test).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mtp3-max-slt-try retries
```

```
default mtp3-max-slt-try
```

- **default**
  
  Resets the number of retries to the default value.

- **retries**
  
  - `retries`: must be an integer between 1 to 65535.
  - Default is 10.

**Usage**

Use this command to troubleshoot MTP3 link mismatch.

**Example**

```
mtp3-max-slt-try 35
```
mtp3-msg-priority

Configures the priority for sending MTP3 management messages.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
mtp3-msg-priority priority
```

default mtp3-msg-priority

```
default
    Resets the number of priority to the default value.
```

```
priority
    priority: must be an integer from 0 to .
    Default is 0.
```

Usage
Use this command to set the priority for sending MTP3 management messages.

Example

```
mtp3-msg-priority 3
```
**mtp3-msg-size**

Configures the size of messages from layer 3 to layer 2.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
  mtp3-msg-size size
  default mtp3-msg-size
```

**Usage**

Use this command to set the maximum message size, in bytes.

**Example**

```
mtp3-msg-size 4096
```
mtp3-p1-qlen

Configure the size for the MTP3 p1 queue length.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

mtp3-p1-qlen size

default mtp3-p1-qlen

default
Rests the number of size of the priority 1 queue to the default value.

size

size: integer from 1 to 65535. Size should be less than MTP3 p2 qlen and p3 qlen. Default is 1024.

Usage

Use this command to configure the queue length threshold for raising the congestion priority to level 1.

Example

mtp3-p1-qlen 128
**mtp3-p2-qlen**

Configure the size of the priority 2 queue.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
**mtp3-p2-qlen** size

default mtp3-p2-qlen
```

**default**
Resets the number of size of the priority 2 queue to the default value.

```
size
size: integer from 1 to 65535. Size should be less than MTP3 p3 qlen and greater than p1 qlen. Default is 1024.
```

**Usage**
Use this command to configure the queue length threshold for raising the congestion priority to level 2.

**Example**
```
mtp3-p2-qlen 256
```
mtp3-p3-qlen

Configure the size of the priority 3 queue.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

mtp3-p3-qlen size

default mtp3-p3-qlen

default
Resets the number of size of the priority 3 queue to the default value.

size

size: integer from 1 to 65535. Size should be greater than MTP3 p1 qlen and p2 qlen . Default is 1024.

Usage
Use this command to configure the queue length threshold for raising the congestion priority to level 3.

Example

mtp3-p3-qlen 1024
mtp3-test-pattern

Configures the character string for the test message.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

mtp3-test-pattern pattern

default mtp3-test-pattern

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the pattern to the default value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>pattern: 1 to 15 alphanumeric characters.</td>
</tr>
<tr>
<td>Default is SGSN-ORIGINATED.</td>
</tr>
</tbody>
</table>

Usage
Use this command to define a test pattern string for the signalling link test match (SLTM).

Example
mtp3-test-pattern TEST1-HomeOffice
priority

Configures the MTP3 Link Priority.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
priority pri_value
no priority
```

- **no**
  - Removes the priority configuration.

- **pri_value**
  - `pri_value`: 0 represents highest priority and 15 represents the lowest priority.

**Usage**

Use this command to configure the link priority within the MTP3 link set.

**Example**

```
priority 2
```
signaling-link-code

Configures the signaling link code (SLC).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
signaling-link-code code
no signaling-link-code
```

**Usage**
Use this command to uniquely identify the signaling link to be used for MTP3 management messages.

**Example**

```
signaling-link-code 4
```
**ssc-f-nni-n1**

Configures the SSCF NNI N1.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
ssc-f-nni-n1 value

no ssc-f-nni-n1
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the ssc-f-nni-n1 configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>value</strong>: integer from 1 to 65535. Default is 1000.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to identify the network-to-node interface (NNI) between the MTP3 and SSCOP layers.

**Example**

```bash
ssc-f-nni-n1 4064
```
sscop-max-cc

Configure the maximum value for the SSCOP connection control (CC) state variable.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sscop-max-cc value
no sscop-max-cc

default
Removes the sscop-max-cc configuration.

value
value: integer from 1 to 65535.
Default is 4.
```

Usage
Use this command as part of the configuration responsible for managing the SSCOP connection. This command sets the number of times retries.

Example

```
sscop-max-cc 256
```
**sscop-max-pd**

Configures the maximum acceptable value for the SSCOP state variable VT(PD).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
sscop-max-pd value
no sscp-max-pd
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the <strong>sscop-max-pd</strong> configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>value: integer from 1 to 65535. Default is 500.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to define the maximum number of data PDUs transmitted between POLL PDUs.

**Example**

```plaintext
sscop-max-pd 2500
```
**sscop-max-stat**

Configures the maximum number of elements included in a status PDU.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sscop-max-stat value
no sscop-max-stat
```

**default**
Removes the sscop-max-stat configuration.

**value**

```
value: integer from 3 to 65535. This parameter should be an odd integer greater than or equal to 3. Default is 67.
```

**Usage**
Received in response to a POLL PDU, the STAT PDU includes information about the number of SD PDUs that have been received.

**Example**

```
sscop-max-stat 56000
```
timeout

This command enables configuration of an array of signaling and flow control timers - for MTP, SSCF, and SSCOP.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

\texttt{timeout \textit{timer}}
\texttt{no \textit{timeout \textit{timer}}}

\texttt{no}

Adding \texttt{no} to the \textit{timeout} command removes the timer configuration.

\texttt{timer}

Repeat the command as needed to configure all required timers.

\begin{itemize}
  \item \texttt{mtp3-tmr-t1} - mtp3 t1 timer, default value is 500ms
  \item \texttt{mtp3-tmr-t12} - mtp3 t12 timer, default value is 800ms
  \item \texttt{mtp3-tmr-t13} - mtp3 t13 timer, default value is 800ms
  \item \texttt{mtp3-tmr-t14} - mtp3 t14 timer, default value is 2000ms
  \item \texttt{mtp3-tmr-t17} - mtp3 t17 timer, default value is 800ms
  \item \texttt{mtp3-tmr-t2} - mtp3 t2 timer, default value is 700ms
  \item \texttt{mtp3-tmr-t22} - mtp3 t22 timer, default value is 180s
  \item \texttt{mtp3-tmr-t23} - mtp3 t23 timer, default value is 180s
  \item \texttt{mtp3-tmr-t24} - mtp3 t24 timer, default value is 500ms
  \item \texttt{mtp3-tmr-t3} - mtp3 t3 timer, default value is 500ms
  \item \texttt{mtp3-tmr-t31} - mtp3 t31 timer, default value is 5s
  \item \texttt{mtp3-tmr-t32} - mtp3 t32 timer, default value is 10s
  \item \texttt{mtp3-tmr-t33} - mtp3 t33 timer, default value is 20s
  \item \texttt{mtp3-tmr-t34} - mtp3 t34 timer, default value is 60s
  \item \texttt{mtp3-tmr-t4} - mtp3 t4 timer, default value is 500ms
  \item \texttt{mtp3-tmr-t5} - mtp3 t5 timer, default value is 500ms
  \item \texttt{mtp3-tmr-t7} - mtp3 t7 timer, default value is 1000ms
  \item \texttt{sscf-nni-tmr-t1} - sscf nni t1 timer. default value is 5s
  \item \texttt{sscf-nni-tmr-t2} - sscf nni t2 timer. default value is 30s
  \item \texttt{sscf-nni-tmr-t3} - sscf nni t2 timer. default value is 10ms
  \item \texttt{sscop-tmr-cc} - sscop cc timer. default value is 200ms
\end{itemize}
• **sscop-tmr-idle** - sscop idle timer (UNI 3.1 only). default value is 100ms
• **sscop-tmr-keep-alive** - sscop keep alive timer. default value is 100ms. For stability purposes, tmrKeepAlive >= tmrPoll and tmrKeepAlive < tmrNoResponse
• **sscop-tmr-no-rsp** - sscop no response timer. default value is 1.5s. For stability purposes, tmrNoResponse > tmrKeepAlive
• **sscop-tmr-poll** - sscop poll timer. default value is 100ms. For stability purposes, tmrPoll <= tmrKeepAlive
Chapter 143
Linkset Configuration Mode Commands

The Linkset configuration mode defines the MTP3 linkset parameters for a specific SS7 routing domain instance.

| Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s). |
adjacent-point-code

This command defines the point-code for the adjacent (next) network element in the SS7 network.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
adjacent-point-code point-code
no adjacent-point-code
```

**point-code**
Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

**no**
Removes the adjacent-point-code configuration for this linkset in the SS7 routing domain.

**Important:** Removing the linkset configuration will result in the termination of all of the links within the linkset.

**Usage**
Use this command to define the point-code for the adjacent element in the SS7 network.

**Example**

```
adjacent-point-code 6.202.7
```
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Returns to the previous mode.
**link**

This command creates an MTP3 link configuration for the SS7 linkset and enters the Link configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
link id id [ link-type [ atm-broadband | highspeed-narrowband | lowspeed-narrowband ] ]
no link id id
```

- **no**
  Disables the specified link configuration.

---

**Important:** Removing the link configuration will result in the termination of traffic on the specified link.

- **_octets**
  Sets the number of octets for the length of the LSSU.

- **id**
  This number uniquely identifies the link in the linkset.
  id: an integer between 1 and 16.

- **link-type**

---

**Important:** This keyword is not yet functional - the feature is still in development.

This keyword is applicable only to releases 8.1 and higher.
Identifies the signalling type for this link; options include:

- atm-broadband
- high speed-narrowband
- low speed-narrowband

**Usage**

Access the Link configuration mode to make changes to the configuration for a link.

**Example**

Access configuration for link 4.
link id 4
**self-point-code**

This command defines the SS7 network point-code to identify this SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
self-point-code  point-code

no self-point-code
```

**point-code**

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.

- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

**no**

Removes the self-point-code configuration for this linkset in the SS7 routing domain.

**Important:** Removing the self-point-code will result in the termination of all traffic on this link.

**Usage**

Use this command to define the SS7 point-code to identify this system.

**Example**

```
self-point-code 6.192.7
```
Chapter 144
LMA Service Configuration Mode Commands

The LMA Service Configuration Mode is used to create and manage the Local Mobility Anchor configuration supporting Proxy Mobile IP on a PDN Gateway in an eHRPD and E-UTRAN/EPC network.

```
Exec Mode
    configure
        Global Configuration Mode
            context name
                Context Configuration Mode
                    lma-service name
                        LMA Service Configuration Mode
```
**aaa accounting**

Enables the LMA to send AAA accounting information for subscriber sessions.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
[ default | no ] aaa accounting
```

- **default**
  Sets the command to the default condition of enabled.

- **no**
  Disables the ability of the LMA to send AAA accounting information.

**Usage**

Use this command to enable the LMA service to send all accounting data (start, stop, and interim) to the configured AAA servers.

**Important:** In order for this command to function properly, AAA accounting must be enabled for the context in which the LMA service is configured using the `aaa accounting subscriber radius` command.

**Example**
The following command disables aaa accounting for the LMA service:

```
no aaa accounting
```
bind address

Binds the LMA service to a logical IP interface serving as the S2a (HSGW) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product
P-GW

Privilege
Administrator

Syntax

bind address ip_address [ max-subscribers num ]

no bind address

no
Removes the interface binding from this service.

ip_address
Specifies the IPv6 address of the interface configured as the S2a or S5/S8 interface. ip_address is specified in colon separated notation.

max-subscribers num
Default: 3000000
Specifies the maximum number of subscribers that can access this service on this interface. num must be configured to an integer between 0 and 3,000,000.

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

Usage
Associate the LMA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to an HSGW (S2a) or S-GW (S5/S8). Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the max-subscribers option, be sure to consider the following:

- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to
Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example
The following command would bind the logical IP interface with the address of 4551::0db8:85a3:08d3:3319:8a2e:0370:1344 to the LMA service and specifies that a maximum of 300,000 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551::0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers 300000
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
refresh-advice-option

Configures inclusion of a refresh advice option in the binding acknowledgement message sent by the LMA.

Product
P-GW

Privilege
Administrator

Syntax

[ default | no ] refresh-advice-option

- **default**
  Returns the command setting to the default setting of disabled.

- **no**
  Disables the inclusion of the refresh advice option in the binding acknowledgement message sent by the LMA

Usage
Use this command to enable the LMA to include this option in a binding acknowledgement sent to the requesting MAG. The option provides a “hint” to the MAG of when it should refresh the binding. As defined in RFC 3775 “Mobility Support in IPv6”, the binding refresh advice option can only be present in the binding acknowledgement sent from the mobile node's home agent in reply to a registration request. A refresh interval parameter determines the amount of time until the mobile node must send a new registration to the home agent to avoid de-registration and loss of session.

**Important**: Refer to the refresh-interval-percent and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.
refresh-interval-percent

Configures percentage of the granted registration lifetime to be used in the refresh interval mobility option in a binding acknowledgement message sent by the LMA service.

Product
P-GW

Privilege
Administrator

Syntax

```
refresh-interval-percent number
default refresh-interval-percent
```

```
default
Resets the command value to the default setting of 75.

number
Default: 75
Sets the percent value for session lifetimes for this service.
number must be an integer value from 1 to 99.
```

Usage

Use this command to configure the amount of the granted registration lifetime to be used in the refresh interval mobility option in the binding acknowledgement message sent by the LMA service to the requesting MAG.

Refreshing a binding or registration is based on the granted registration lifetime. Since a refresh request must be within the granted range of a registration lifetime, this command provides a method of setting the interval of when a refresh request is sent.

As described in RFC 3775 “Mobility Support in IPv6”, if a binding refresh advice option is present in the binding acknowledgement, the refresh interval field in the option must be a value less than the binding lifetime (also returned in the binding acknowledgement). The mobile node then should attempt to refresh its registration at the shorter refresh interval. The home agent will still honor the registration for the lifetime period, even if the mobile node does not refresh its registration within the refresh period.

Important: Refer to the refresh-advice-option and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

Example

The following command sets the refresh interval percent to 90:

```
refresh-interval-percent 90
```
reg-lifetime

Configures the Mobile IPv6 session registration lifetime for this service.

Product
P-GW

Privilege
Administrator

Syntax

reg-lifetime seconds

default reg-lifetime

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the command value to the default setting of 600.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 600</td>
</tr>
<tr>
<td>Sets the time value for session lifetimes for this service.</td>
</tr>
<tr>
<td>seconds must be an integer value from 1 to 262140.</td>
</tr>
</tbody>
</table>

Usage
Use this command to limit PMIPv6 lifetime on this service. If the PBU contains a lifetime shorter than what is specified, it is granted. If the lifetime is longer, then HA service will limit the granted lifetime to the configured value.

Important: Refer to the refresh-interval-percent and refresh-advice-option commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

Example
The following command sets the registration lifetime for Mobile IPv6 sessions using this service to 1200 seconds (20 minutes):

    reg-lifetime 1200
revocation

Enables the MIP revocation feature and configures revocation parameters.

Product: P-GW
Privilege: Administrator

Syntax:

- `revocation { enable | max-retransmission number | retransmission-timeout msecs }`
- `default revocation { enable | max-retransmission | retransmission-timeout }
- `no revocation enable`  

- `default`
  Resets the keyword to its default value.

- `no`
  Disables revocation for this service.

- `enable`
  Default: disabled
  Enables the MIP registration revocation feature for the LMA service. When enabled, if revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a Revocation message to the MAG. This feature is disabled by default.

- `max-retransmission number`
  Default: 3
  The maximum number of retransmissions of a Revocation message before the revocation fails. `number` must be an integer value from 0 through 10.

- `retransmission-timeout msecs`
  Default: 3000
  The number of milliseconds to wait for a Revocation Acknowledgement from the MAG before retransmitting the Revocation message. `msecs` must be an integer value from 500 through 10000.

Usage:

Use this command to enable or disable the MIP revocation feature on the LMA or to change settings for this feature.

Example:

The following command sets the maximum number of retries for a Revocation message to 6:
The following command sets the timeout between retransmissions to 10:

```
revocation retransmission-timeout 10
```
sequence-number-validate

Confirms sequence number validation of the received MIPv6 control packets by the LMA service according to RFC 3775.

**Product**

P-GW

**Privilege**

Administrator

**Syntax**

[ default | no ] sequence-number-validate

**default**

Resets the command value to the default setting of enabled.

**no**

Disables the feature.

**Usage**

Use this command to configure the sequence number validation of the received MIPv6 control packets (PBUs) by the LMA service. This feature validates MIPv6 control packets and insures that any incoming packets with a sequence number prior to the last number received is consider invalid. If this service has no cache entry of the home address included in the PBU, it will accept any sequence value in the initial PBU from the mobile node.
setup-timeout

The maximum amount of time allowed for session setup.

Product
P-GW

Privilege
Administrator

Syntax

```
setup-timeout seconds

default setup-timeout
```

```
default

 Resets the command value to the default setting of 60.

 seconds

 Default: 60 seconds

 The maximum amount of time, in seconds, to allow for setup of a session in this service. `seconds` must be an integer value from 1 through 1000000.
```

Usage

Use this command to set the maximum amount of time allowed for setting up a session.

Example

The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

```
setup-timeout 300
```
timestamp-replay-protection

Designates timestamp replay protection scheme as per RFC 4285.

Product
P-GW

Privilege
Administrator

Syntax

```
timestamp-replay-protection tolerance seconds

[ default | no ] timestamp-replay-protection tolerance
```

```
default
Resets the command value to the default setting of 7.

no
Disables the timestamp replay protection feature.

seconds
Default: 7
Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds.
seconds must be an integer value between 0 and 65535.
```

Usage

Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.

Example

The following command sets the acceptable difference for timestamps to 10 seconds:

```
timestamp-replay-protection tolerance 10
```
The LNS Service Configuration Mode is used to create and manage L2TP services within contexts on the system. LNS services facilitate tunneling with peer LACs.

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

Enables the sending of AAA accounting information by the LNS.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

[no] aaa accounting

no

Disables this option.

Usage
Use this command to enable the sending of AAA accounting information by the LNS. By default this is enabled.

Example
The following command enables the sending of AAA accounting information by the LNS:

aaa accounting
authentication

Configures the type of subscriber authentication for PPP sessions terminated at the current LNS.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
authentication { [ [ allow-noauth ] [ chap chap_priority ] [ mschap mschap_priority ] [ pap pap_priority ] ] | msid-auth }
```

**allow-noauth**

Default: Disabled
This option configures the LNS to allow PPP sessions access even though they have not been authenticated.
This command issued by itself causes the LNS to not attempt authentication for any PPP sessions.
When the allow-noauth option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system will treat the allow-noauth option as the lowest priority.
If no authentication is allowed, then NAI construct will be implemented in order to provide accounting records for the PPP session.

**chap  chap_priority**

Default: 1
This option configures the LNS to attempt to use the Challenge Handshake Authentication Protocol (CHAP) to authenticate the PPP session.
A *chap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
*chap_priority* must be an integer from 1 through 1000. The lower the integer, the higher the preference.
CHAP is enabled by default as the highest preference.

**mschap  mschap_priority**

Default: Disabled
This option configures the LNS to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the PP session.
A *mschap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
*mschap_priority* must be an integer from 1 through 1000. The lower the integer, the higher the preference.

**pap  pap_priority**

Default: 2
This option configures the LNS to attempt to use the Password Authentication Protocol (PAP) to authenticate the PPP session.
A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
**authentication**

`pap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

**msid-auth**

Default: Disabled
This option configures the LNS to attempt to authenticate the PPP session based on the Mobile Station Identity (MSID).

**Usage**

Use to specify how the LNS service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.

The chassis is shipped from the factory with the LNS authentication options set as follows:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

**Important:** At least one of the keywords must be used to complete the command.

**Example**

The following command configures the LNS service to allow no authentication for PPP sessions and would perform accounting using the default NAI-construct of username@domain:

```
authentication allow-noauth
```

The following command configures the system to attempt authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, when all attempts to authenticate the subscriber using these protocols failed, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```
avp map called-number apn

This command maps an incoming AVP to a GGSN APN for authentication and authorization of the call.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
{ default | no } avp map called-number apn
```

**Usage**
For LNS calls received through a LAC, the ICRQ message includes an APN name in the Called Number AVP. This mapping function enables a GGSN system to provide RADIUS authentication/authorization via a defined APN in place of an LNS configuration. If the mapped APN has not been defined within the GGSN configuration then the call will be rejected.

**Example**
Enter the following command to enable mapping:

```
avp map called-number apn
```

Enter the following command to disable mapping:

```
no avp map called-number apn
```
bind

This command assigns the IP address of an interface in the current context to the LNS service.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

bind ip_address  [max-subscribers max_value ]
no bind ip_address

no
Unassign, or unbind, the local end point to the LNS service.

ip_address
The IP address of an interface in the current context. This must be a valid IPv4 address, using dotted-decimal notation.

max-subscribers max_value
Default: 10000
The maximum number of subscribers that can be connected to this service at any time. max_value must be an integer from 1 through 2500000.

Usage
Use this command to bind the IP address of an interface in the current context to the LNS service.

Example
The following command binds the current context interface IP address 192.168.100.10 to the current LNS service:

bind 192.168.100.10

The following command removes the binding of the IP address from the LNS service:

no bind
data sequence-number

Enables data sequence numbering for sessions that use the current LNS service. Data sequence numbering is enabled by default.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] data sequence-number
```

- **no**
  Disables data sequence numbering for sessions.

**Usage**
An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

**Example**
Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```
default

This command sets the specified LAC service parameter to its default value or setting.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

default { authentication | data sequence-number | ip source-violation | keepalive-interval | load-balancing | local-receive-window | max-retransmission | max-session-per-tunnel | max-tunnel-challenge-length | max-tunnels | proxy-lcp-authentication | retransmission-timeout-first | retransmission-timeout-max | setup-timeout | single-port-mode | subscriber | trap all tunnel-authentication}

authentication

Sets the authentication parameters for PPP sessions to the following defaults:
- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

data sequence-number

Enables data sequence numbering for sessions.

ip source-violation

Sets the IP source violation parameters to the following defaults:
- drop-limit 10
- period 120 seconds
- reneg-limit 5

keepalive-interval

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 secs.

local-receive-window

Sets the window size to be used for the local side for the reliable control transport to the default of 4.

max-retransmission

Sets the maximum number of retransmissions to the default of 5.
max-session-per-tunnel
Sets the maximum number of sessions per tunnel at any point in time to the default of 65535.

max-tunnel-challenge-length
Sets the maximum length of the tunnel challenge to the default of 16 bytes.

max-tunnels
Sets the maximum number of tunnels for this service to the default of 32000.

proxy-lcp-authentication
Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first
Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max
Sets the maximum retransmit interval to the default of 8 seconds.

setup-timeout
Sets the maximum time allowed for session setup to the default of 60 seconds.

single-port-mode
Disables assignment of only port 1107 for incoming tunnels and allows dynamic assignment of ports.

subscriber
Sets the name of the default subscriber configuration to use.

tunnel-authentication
Sets tunnel authentication to the default state of enabled.

trap all
Generates all supported SNMP traps.

tunnel-switching
Sets the ability of the LNS to create subsequent tunnels to the default of enabled.

Usage
Use the default command to set LAC service parameters to their default states.

Example
Use the following command to set the keep alive interval to the default value of 60 seconds:

default keepalive-interval
Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

```
default max-session-per-tunnel
```
ip source-violation

This command configures settings related to IP source-violation detection.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num }
```

```
o ip source-violation clear-on-valid-packet
```

---

**clear-on-valid-packet**

Default: disabled
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

**drop-limit** num

Default: 10
Sets the number of allowed source violations within a detection period before forcing a call disconnect. If num is not specified, the value is set to the default.
num can be any integer value from 1 to 1000000.

**period** secs

Default: 120
The length of time, in seconds, for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.
The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If secs is not specified, the value is set to the default.
secs can be any integer value from 1 to 1000000.

**reneg-limit** num

Default: 5
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If num is not specified, the value is set to the default.
num can be any integer value from 1 to 1000000.

---

**Usage**

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDSNs a number of times during a handoff scenario.
This function operates in the following manner:
When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.

If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.

If at any time before the call is dropped, the configured source-violation period is exceeded, the counters for drop-limit is decremented by half and reneg-limit is decremented by 1. See period definition above.

Example
To set the maximum number of source violations before dropping a call to 100, enter the following command:

```
ip source-violation drop-limit 100
```
keepalive-interval

This command specifies the amount of time to wait before sending a Hello keep alive message.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
keepalive-interval seconds
no keepalive-interval

seconds
```

Disables the generation of Hello keep alive messages on the tunnel.

Usage

Use this command to set the amount of time to wait before sending a Hello keep alive message or disable the generation of Hello keep alive messages completely. A keep alive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example

Use the following command to set the Hello keep alive message interval to 120 seconds:
```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keep alive messages:
```
nocfg
```

Keepalive-Interval
local-receive-window

Specifies the number of control messages the remote peer LAC can send before waiting for an acknowledgement.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
local-receive-window integer
```

*integer*
Default: 4
The number of control messages to send before waiting for an acknowledgement. The number can be configured to any integer value from 1 through 256.

Usage
Use this command to set the size of the control message receive window being offered to the remote peer LAC. The remote peer LAC may send the specified number of control messages before it must wait for an acknowledgment.

Example
The following command sets the local receive window to 10 control messages:

```
local-receive-window 10
```
max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
max-retransmission integer
```

```
ing \textit{integer}

Default: 5
The maximum number of retransmissions of a control message to a peer. This value must be an integer from 1 through 10.
```

Usage

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.
Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within it.

Example

The following command sets the maximum number of retransmissions of a control message to a peer to 7:

```
max-retransmissions 7
```
max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single tunnel at any time.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
max-sessions-per-tunnel integer
```

- **integer**
  - Default: 512
  - The maximum number of sessions. This value must be from 1 through 65535.

**Usage**
Use this command to set the maximum number of sessions you want to allow in a tunnel.

**Example**
The following command sets the maximum number of sessions in a tunnel to 5000:

```
max-sessions-per-tunnel 5000
```
max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes. The challenge is used for tunnel authentication purposes during tunnel creation.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
max-tunnel-challenge-length bytes
```

**bytes**
Default: 16
The number of bytes to set the maximum length of the tunnel challenge. This must be a value from 4 through 32.

Usage
Use this command to set the maximum length, in bytes, for the tunnel challenge that is used during tunnel creation.

Example
The following command sets the maximum length of the tunnel challenge to 32 bytes:
```
max-tunnel-challenge-length 32
```
max-tunnels

The maximum number of tunnels that the current LNS service can support.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
max-tunnels integer
```

- `integer`
  
  Default: 32000
  
  The maximum number of tunnels. This value must be an integer from 1 to 32000.

**Usage**

Use this command to set the maximum number of tunnels that this LNS service can support at any one time.

**Example**

Use the following command to set the maximum number of tunnels for the current LNS service to 20000:

```
max-tunnels 20000
```
nai-construction domain

Designates the alias domain name to use for Network Access Identifier (NAI) construction.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
no nai-construction-domain
```

```
domain_name { @ | % | - | \ | # | / }
```

The desired domain name alias followed immediately by a separator from the valid list. `domain_name` must be a string of from 1 through 79 alphanumeric characters.

Usage
Use this command to specify the domain alias and separator to use for NAI construction. The specified domain name must be followed by a valid separator (@ | % | - | \ | # | /).

Example
To specify a domain alias of mydomain with a separator of @, enter the following command:
```
nai-construction-domain mydomain@
```
To delete the current setting for the NAI construction domain alias, enter the following command:
```
no nai-construction-domain
```
peer-lac

Adds a peer LAC address for the current LNS service. Up to 8 peer LACs can be configured for each LNS service.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
peer-lac {ip_address | ip_address/mask} [encrypted] secret secret [description text]
no peer-lac ip_address
```

**no peer-lac ip_address**
Deletes the peer LAC IP address specified by `ip_address`. `ip_address` must be entered in standard IPv4 dotted decimal notation.

**ip_address**
The IP address of a specific peer LAC for the current LNS service. `ip_address` must be entered in standard IPv4 dotted decimal notation.

**ip_address/mask**
A network prefix and mask enabling communication with a group of peer LACs. `ip_address` is the network prefix expressed in dotted decimal notation. `mask` is the number of bits that defines the prefix.

**[encrypted]**
Specifies the encrypted shared key between the LAC and the LNS service. This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

**secret secret**
Designates the secret which is shared between the current LNS service and the peer LAC. `secret` must be a string from 1 to 127 alpha and/or numeric characters and is case sensitive.

**description text**
Specifies the descriptive text to use to describe the specified peer LAC. `text` must be 0 to 79 alpha and/or numeric characters with no spaces or a quoted string of printable characters.

**Usage**

Use this command to add a peer LAC address for the current LNS service. Specific peer LACs can be configured by specifying their individual IP addresses. In addition, to simplify configuration, communication with a group of peer LACs can be enabled by specifying a network prefix and a mask.
Example
The following command adds a peer LAC to the current LNS service with the IP address of 10.10.10.100, and specifies the shared secret to be 1b34nnf5d:
peer-lac 10.10.10.100 secret 1b34nnf5d
The following command enables communication with up to 16 peer LACs on the 192.168.1.0 network each having a secret of abc123:
peer-lac 192.168.1.0/28 secret abc123
The following command removes the peer LAC with the IP address of 10.10.10.200 for the current LNS service:
no peer-lac 10.10.10.200
### proxy-lcp-authentication

Enables/disables proxy LCP authentication.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy-lcp-authentication</td>
<td>Enables the processing proxy LCP authentication parameters from the LAC.</td>
</tr>
<tr>
<td>no proxy-lcp-authentication</td>
<td>Disables the processing of proxy LCP authentication parameters from the LAC.</td>
</tr>
</tbody>
</table>

**Usage**

When enabled, if proxy LCP authentication parameters are received from the LAC and are acceptable, the LNS resumes the PPP session from the authentication phase and goes to the IPCP phase. When disabled, PPP is always started from the LCP phase, ignoring and discarding any proxy LCP authentication parameters received from the LAC. Disable this feature in situations where accept proxy LCP Auth AVPs that the peer LAC sends should not be expected.

**Example**

Use the following command to disable the processing of proxy LCP authentication parameters from the LAC:

```plaintext
no proxy-lcp-authentication
```

Use the following command to re-enable the processing of proxy LCP authentication parameters from the LAC:

```plaintext
proxy-lcp-authentication
```
retransmission-timeout-first

Configures the initial timeout for the retransmission of control messages to the peer LAC.

Privilege
Security Administrator, Administrator

Syntax
```
retransmission-timeout-first integer
```

integer
Default: 1
The amount of time to wait before sending the first control message retransmission. This value is measured in seconds and must be an integer from 1 to 100.

Usage
Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted.

Example
The following command sets the initial retransmission timeout to 3 seconds:
```
retransmission-timeout-first 3
```
retransmission-timeout-max

Configures the maximum amount of time that can elapse before retransmitting control messages to the peer LAC.

Privilege
Security Administrator, Administrator

Syntax
```
retransmission-timeout-max integer
```

integer
Default: 8
The maximum time to wait before retransmitting control messages. If this limit is reached, the tunnel, and all sessions within it, is cleared. This value is measured in seconds and must be an integer in the range of 1 to 100.

Usage
Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. This continues until the limit set by this command is reached. If this limit is reached, the tunnel, and all sessions within it, is cleared.

Example
Use the following command to set the maximum retransmission time-out to 10 seconds:
```
retransmission-timeout-max 10
```
setup-timeout

Configures the maximum amount of time, in seconds, allowed for session setup.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
setup-timeout seconds
```

seconds
Default: 60
The maximum time to wait, in seconds, for the setup of a session. seconds must be an integer from 1 through 1000000.

Usage
This command controls the amount of time allowed for tunnel establishment with a peer LAC. If this timer is exceeded the tunnel setup is aborted.

Example
The following command configures a maximum setup time of 120 seconds:

```
setup-timeout 120
```
**single-port-mode**

When enabled, this command sets the LNS to use only the default local UDP port (port 1701) for the life of a tunnel.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>single-port-mode</code></td>
<td>Enable single port mode</td>
</tr>
<tr>
<td><code>no single-port-mode default single-port-mode</code></td>
<td>Disable single port mode</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Disable single port mode</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to control the L2TP LNS tunnel local UDP port assignment mode. If single-port-mode is enabled, the LNS-service uses the standard UDP port (port 1701) for the life of the incoming tunnel. Otherwise, it assigns a new local UDP port number for a tunnel when it responds to a tunnel create request received on the standard port number. This is done for load distributing the tunnel processing between multiple tasks within the system to increase the capacity and performance. Even though all L2TP LACs are required to support such dynamic port assignments during tunnel establishments, there exist some LACs that do not support port assignment other than port 1701. This single-port-mode feature can be enabled to support such LAC peers. This configuration must be applied for the LNS-Service before the `R_bind` command is executed.

**Example**

The following command enables single port mode for the current LNS service:

```
single-port-mode
```
**trap**

This command generates SNMP traps.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
trap all  
no trap all
```

Use this command to enable/disable all supported SNMP traps.

**Example**

To enable all supported SNMP traps, enter the following command:

```
trap all
```
**tunnel-authentication**

Enables/disables L2TP tunnel authentication for the LNS service.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
tunnel-authentication
no tunnel-authentication

no
```

Disables tunnel authentication
Tunnel authentication is enabled by default.

**Usage**

When tunnel authentication is enabled, a configured shared secret is used to ensure that the LNS service is communicating with an authorized peer LAC. The shared secret is configured by the `R_peer-lac` command, the `R_tunnel l2tp` command in the Subscriber Configuration mode, or the `Tunnel-Password` attribute in the subscribers RADIUS profile.

**Example**

To disable tunnel authentication, use the following command:
```
no tunnel-authentication
```

To re-enable tunnel authentication, use the following command:
```
tunnel-authentication
```
tunnel-switching

Enables/disables the LNS service from creating tunnels to another LAC for an existing tunnel.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
tunnel-switching
no tunnel-switching
```

```
no

Disable tunnel switching.
Tunnel switching is enabled by default.
```

**Usage**

Tunnel switching is when the LNS has a tunnel connected to a LAC and creates a tunnel to a different LAC and routes the data from the original LAC through the new tunnel to the other LAC.

**Example**

To disable tunnel switching in the LNS, enter the following command;

```
no tunnel-switching
```
The Loopback Interface Configuration Mode is used to create and manage loopback interfaces that provide IP addresses that are always available and reachable from any interface within the same given context.

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

Configures the description text for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
description text
no description
```

- **no**
  Clears the description for the interface.

- **text**
  Specifies the descriptive text to use. `text` must be 0 to 79 alpha and/or numeric characters with no spaces or a quoted string of printable characters

Usage

Set the description to provide useful information on the interface’s primary function, services, end users, etc. Any information useful may be provided.

Example

description sampleInterfaceDescriptiveText
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the interface configuration mode and returns to the context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the context configuration mode.
ip address

Configures the IP options for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip address {ip_address/ip_mask | ip_address/bitmask} [secondary | srp-activate]
o ip address ip_address
```

no ip address ip_address

no
Deletes the specified IP address from the interface configuration.

```
address {ip_address/ip_mask | ip_address/bitmask} [secondary | srp-activate]
```

Configures the IP address and network mask for the interface.

- `ip_address/ip_mask` specifies an IP address and the subnet mask pair which is used to identify the IP address of the interface. `ip_address` must be specified using the standard IPv4 dotted decimal notation. Currently, the only value accepted for ip_mask is 255.255.255.255.
- `ip_address/net_mask`: the IP address and the length in bits of the network mask. This must be an IP address entered in dotted decimal notation and a mask (192.168.1.0/32). Currently, the only value accepted for bit_mask is 32.

The `secondary` keyword is used to configure a secondary IP address on the interface. This is referred to as multi-homing of the interface.

The `srp-activate` keyword activates the IP address for Interchassis Session Redundancy.

Usage

Create and manage loopback interfaces for the current context.

Example

The following command configures IP address to associate with the interface:

```
ip address 1.2.3.4 255.255.255.255
```

The following command removes the associated IP address for the interface:

```
no ip address 1.2.3.4
```
ip vrf

This command configures the IP VPN Routing/Forwarding instance for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip vrf forwarding vrf_name
no vrf forwarding
```

no

Deletes the specified IP VPN routing/forwarding instance from the interface configuration.

```
vrf_name
```

Specifies the preconfigured IP VPN routing/forwarding instance name which is to be used with this interface. `vrf_name` must be a preconfigured VPN routing/forwarding instance name with `ip vrf forwarding` command in Context Configuration Mode.

Usage

Use this command to associate a preconfigured IP VPN Routing/Forwarding instance for the current interface.

Example

The following command associates a preconfigured IP routing/forwarding instance named `vrf_1` with this interface:

```
ip vrf forwarding vrf_1
```
ipv6 address

Configures the IPv6 options for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ipv6 address ipv6_address ip_mask [ srp-activate ]
no ipv6 address ipv6_address

no
Deletes the specified IPv6 address from the interface configuration.

address ipv6_address ip_mask [ srp-activate ]
Configures the IP address and network mask for the interface.
ipv6_address ip_mask specifies an IP address and the subnet mask pair which is used to identify the IPv6 address of the interface. ipv6_address must be specified using the standard IPv6 dotted decimal notation.
The srp-activate keyword activates the IPv6 address for Session Recovery.

Usage
Create and manage loopback interfaces for the current context and enable Session Redundancy Protocol (SRP) when appropriate.

Example
The following command configures an IPv6 address to associate with the interface and enables SRP:

ipv6 address 2001:268:2008::1021/128 srp-activate
Chapter 147
MAG Service Configuration Mode Commands

The MAG Service Configuration Mode is used to create and manage a Mobility Access Gateway service in an HSGW (eHRPD network) or a P-MIP S-GW (LTE-SAE network). The MAG is the PMIP client and communicates with the Local Mobility Anchor (LMA) configured on a PDN Gateway.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

mag-service name

MAG Service Configuration Mode
```
**bind address**

Binds the service to a logical IP interface serving as the S2a (HSGW) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

**Product**
HSGW, S-GW

**Privilege**
Administrator

**Syntax**

```plaintext
bind address ip_address [ max-subscribers num ]
```

**no bind address**

---

**no**
Removes the interface binding from this service.

**ip_address**
Specifies the IPv6 address of the interface configured as the S5/S8 interface. `ip_address` is specified in colon separated notation.

**max-subscribers num**
Default: 1500000
Specifies the maximum number of subscribers that can access this service on this interface. `num` must be configured to an integer between 0 and 3000000.

---

**Important:** The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

**Usage**

Associate the MAG service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to/from a PDN gateway. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the `max-subscribers` option, be sure to consider the following:
- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to
Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

**Example**
The following command would bind the logical IP interface with the address of 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 to the MAG service and specifies that a maximum of 300,000 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers 300000
```
encapsulation

Configures data encapsulation type to be used for specific MAG service.

Product
HSGW, S-GW

Privilege
Administrator

Syntax

encapsulation { gre | ipip }
default encapsulation

default
Resets the encapsulation type to be used by this service to the default option of GRE.

{ gre | ipip }
gre: Specifies that GRE encapsulation is to be used for PMIPv6 tunnel data between the MAG and the LMA. This is the default for this command.
ipip: Specifies that IP-in-IP encapsulation is to be used for PMIPv6 tunnel data between the MAG and the LMA.

Usage
Use this command to select the encapsulation type to be used for PMIPv6 tunnel data between the MAG and the LMA.

Example
The following command sets the encapsulation data to IP-in-IP:

encapsulation ipip
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Administrator

Syntax
exit

Usage
Return to the previous mode.
information-element-set

Identifies the information element set of mobility options to be used in Proxy Binding Update (PBU) messages sent by the MAG to the LMA.

Product
HSGW, S-GW

Privilege
Administrator

Syntax

information-element-set { custom1 | standard }

default information-element-set

default

Resets the command to the default value of “standard”.

{ custom1 | standard }

custom1: Specifies that a custom set of mobility options to be used in proxy binding update messages that are sent in Vendor Specific Mobility Options. These options are:
• User Location Info
• Hardware Identifier
• Access Network Charging Identifier

standard: Specifies that a standard set of mobility options are to be used in proxy binding update messages. The 3GPP specification, 29.275 defines these as Protocol Configuration Options.

Usage

Use this command to identify the type of information element set of mobility options to be used in PBU messages sent from the MAG to the LMA. The mobility options can be either standards-based (3GPP 29.275) or custom (vendor-specific as defined by 3GPP 29.275).

Example

The following command identifies the information element set of mobility options to use in PBU messages as custom:

information-element-set custom1
max-retransmissions

Configures maximum number of retransmissions of Proxy MIP control messages to the LMA.

**Product**
HSGW, S-GW

**Privilege**
Administrator

**Syntax**

```
max-retransmissions num

default max-retransmissions
```

**default**
Rests the maximum number of allowed retransmissions to the default value of 5.

**num**
Default: 5
Specifies the maximum number of times the MAG service will attempt to communicate with the LMA before it marks it as unreachable. count can be configured to any integer value between 1 and 4294967295.

**Usage**
Use this command to limit the number of retransmissions to LMA before marking it as unreachable. If the value configured is reached, the call is dropped.

**Example**
The following command configures the maximum number of retransmissions for the MAG service to 3:

```
max-retransmissions 3
```
**reg-lifetime**

Configures the Mobile IPv6 session registration lifetime for this service.

**Product**
HSGW, S-GW

**Privilege**
Administrator

**Syntax**

```plaintext
reg-lifetime seconds
```

**default reg-lifetime**

```plaintext
default
```

Reset the command value to the default setting of 600.

```plaintext
seconds
```

Default: 600
Sets the time value for session lifetimes for this service.

*seconds* must be an integer value from 1 to 262140.

**Usage**

Use this command to limit PMIPv6 lifetime on this service. If the PBA from the LMA contains a lifetime shorter or longer than what is specified, it is used instead.

**Example**

The following command sets the registration lifetime for Mobile IPv6 sessions using this service to 1200 seconds (20 minutes):

```plaintext
reg-lifetime 1200
```
renew-percent-time

Configures percentage of lifetime at which a registration renewal is sent to the LMA.

Product
HSGW, S-GW

Privilege
Administrator

Syntax

```
renew-percent-time percent
default renew-percent-time
```

default
Resets the command to the default value of 75.

percent
Default: 75
Specifies the time when the registration renewal is sent to the LMA. `percent` is a percentage value of the registration lifetime and must be an integer value from 1 to 100.

Usage
Use this command to specify when a registration renewal is sent to the LMA for subscribers using this service.
If the registration lifetime is 600 seconds (10 minutes) and this command is set to 75 (percent), then the registration renewal message is sent after 450 seconds of the registration lifetime has expired.

Example
The following command sets the registration renewal time for subscribers using this service to 90 percent of the registration lifetime:

```
renew-percent-time 90
```
retransmission-policy

Configures the retransmission policy for Proxy MIP control message retransmissions.

Product
HSGW

Privilege
Administrator

Syntax

retransmission-policy { exponential-backoff | normal }

default retransmission-policy

- default
  Returns the command to its default setting of exponential-backoff.

{ exponential-backoff | normal }

- exponential-backoff
  Specifies that the Proxy Binding Update retransmission uses an exponential backoff to increase the retransmission timeout for each retry.

- normal
  Specifies that the Proxy Binding Update retransmission uses the configured retransmission timeout value for all PBU retransmission retries.

Usage

Use this command to specify the retransmission policy for PMIP control messages.

Example

The following command sets the retransmission timeout policy for PMIP control packets to “normal”:

retransmission-policy normal
retransmission-timeout

Configures the maximum allowable time for the MAG service to wait for a response from the LMA before it attempts to communicate with the LMA again (if the system is configured to retry the LMA) or marks the LMA as unreachable.

Product
HSGW, S-GW

Privilege
Administrator

Syntax

retransmission-timeout time

{ default | no } retransmission-timeout

default
Resets the timeout setting to the default value of 3.

no
Deletes a previously configured timeout value.

time
Default: 3 seconds (300)
Specifies the maximum allowable time, in milliseconds, for the MAG service to wait for a response from the LMA before it: a) attempts to communicate with the LMA again (if the system is configured to retry the LMA) or b) marks the LMA as unreachable.
time must be an integer value between 100 and 100000.

Usage
Use the retransmission timeout command in conjunction with the max-retransmissions command in order to configure the MAG services behavior when it does not receive a response from a particular LMA.

Example
The following command configures a retransmission timeout value of 5 seconds:

retransmission-timeout 5
Chapter 148
MAP Service Configuration Mode Commands

The MAP Service Configuration Mode is used to configure properties for Mobile Application Part (MAP) service. Mobile Application Part (MAP) is a protocol which provides an application layer for the various nodes in the core mobile network and GPRS and UMTS core network to communicate with each other in order to provide services to mobile phone users. The MAP service provides the application-layer protocol support used to access the Home Location Register (HLR).

---

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

Configures access protocol parameters for the MAP service as defined for a specific SCCP network instance.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
access-protocol sccp-network sccp_id
no access-protocol

sccp-network sccp_id
Specifies the ID number of the SCCP network to use for the SGSN connection.
sccp_id: Must be an integer from 1 to 16.

no
Removes the access protocol SCCP network instance ID from the configuration.
```

**Usage**
Use this command to associate access protocol parameters to a specific instance of the MAP service for an SCCP network.

**Example**
The following command associates the access protocols with the SCCP network ID #10:

```plaintext
access-protocol sccp-network 10
```
**application-context-name**

Configure the operation timer(s) for one or more MAP application contexts.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
application-context-name application operation-timer value
default application-context-name application operation-timer
```

**default**

Resets the operation timers for all applications to system defaults.

**application**

Select one of the following applications to enable the application:

- **authentication-failure-report**: Sets the reporting operation timer for authentication failure. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **cancel-location**: Sets the cancel location operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **check-imei**: Sets the check-IMEI operation timer. The setting range for this timer is 15 to 30 seconds for releases 8.0 and 8.1 and 1 to 30 seconds for releases 9.0 and higher. The default setting is 15 seconds.
- **delete-subscriber-data**: Sets the delete subscriber data operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mo-fwd-sm**: Sets the operation timer for forwarding mobile-originated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ms-purge**: Sets the operation timer for MS-purge function. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mt-fwd-sm**: Sets the operation timer for forwarding mobile-terminated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ready-for-sm**: Sets the operation timer for the ready for SMS operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **send-authentication-info**: Sets the operation timer for the sending authentication information operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **stand-alone-insert-subscriber-data**: Sets the operation timer for the standalone insert subscriber data operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
• **ugl-insert-subscriber-data**: Sets the operation timer for the insert subscriber data portion of the update GPRS location operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

• **update-gprs-location**: Sets the operation timer for the update GPRS location operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

```plaintext
operation-timer value
```

Configures the operation timer for the selected application. Timer values are indicated above.

**Usage**

Repeat this command entering a different application each time to enable multiple applications.

**Example**

```plaintext
application-context-name stand-alone-insert-subscriber-data operation-timer operation-timer 20
```
auth-vectors

Configures the number of authorization vectors to be requested from the home location register (HLR) during call setup to provide subscriber authentication.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
auth-vectors number-to-request number

default auth-vectors number-to-request
```

- **default**
  Resets the number of vectors requested from the HLR to the system default.

- **number-to-request number**
  
  `number`: Must be an integer from 1 to 5 to define the number of authorization vectors be requested from the HLR.
  Default is 5.

**Usage**

Set the number of requests to be received from the HLR.

**Example**

```
auth-vectors number-to-request 4
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
equipment-identity-register

Defines the address of the equipment-identity-register (EIR) used by the SGSN.

Product  
SGSN

Privilege  
Security Administrator, Administrator

Syntax

equipment-identity-register { isdn E.164_num | point code pt_code } [ source-ssn ssn | checkimei-every-n-events times]

no equipment-identity-register { isdn E.164_num | point codept_code }

no

Deletes the EIR configuration.

isdn number

Enter the E.164 number of the EIR.

number: must be a string of 1 to 15 digits.

point code pt_code

Enter SS7 point code address of the EIR in dotted-decimal format according to variant settings:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- or a string of 1 to 11 characters

source-ssn ssn

Identifies the subsystem number (SSN) to be used.

ssn must be an integer from 1 to 255.

checkimei-every-n-events times

Configures the frequency with which a ‘check IMEI’ message is sent to the EIR. When set, the SGSN skips sending the ‘check IMEI’ message for the first N-1 received attach requests.

times must be an integer from 1 to 15.

Important: This feature must be enabled by enabling verify-equipment-identity in the gmm retrieve-equipment-identity imei command of the SGSN Operator Policy configuration mode.

Usage

Configure the identity of the EIR that the SGSN uses and the interaction parameters.
Example

equipment-identity-register point code 7.255.7
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the context configuration mode.
This command enters the configuration mode for the home location register (HLR). The HLR is a database containing the subscriber profile information for all mobile stations (MS) / user equipment (UE) connecting to a specific GPRS or UMTS core network.

**Important:** The commands and options for this mode are documented in the HLR Configuration Mode chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
hlr
```
policy

This command configures the Transaction Capabilities Application Part (TCAP) -specific MAP policy for either ANSI or ITU SS7 variants.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ default ] policy tcap { use-received-destination-address | use-received-source-address }

use-received-destination-address
Selecting this keyword overwrites stored CG and CD addresses with a new address received in first TC CNT msg

use-received-source-address
Selecting this keyword instructs the MAP service to use the received source address for the dialog.

Usage
Use this command to determine how TCAP will handle MAP messages.

Example

policy tcap use-received-destination-address
short-message-service

This command enables and disables the short message service (SMS service) and provides access to the SMS service configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

\[
\text{[ no ] short-message-service}
\]

\[
\text{no}
\]

Disables the SMS service.

**Usage**
Enter the command to access the SMS service configuration mode to fine tune the SMS functionality.

**Example**

short-message-service
Chapter 149
MIP HA Assignment Table Configuration Mode Commands

The Mobile IP HA Assignment Table Configuration Mode is used to assign specific HA IP addresses to ranges of Mobile Node IP addresses.
end

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

**Product**

PDSN, HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
end
```

**Usage**

Returns to the Exec mode.
exit

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

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Return to the Context Configuration mode.
hoa-range

This command assigns ranges of Mobile Node (MN) IP addresses to specific Home agent IP addresses.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

hoa-range ip_address ip_address2 ha ip_address3
no hoa-range ip_address ip_address2 ha ip_address3

no
Remove the specified Home Agent assignment from the assignment table.

ip_address ip_address2
Specifies a range of MN IP addresses. ip_address and ip_address2 must be specified in either IPv4 dotted decimal notation or IPv6 colon notation.

ha ip_address3
Specifies the IP address of the Home Agent to assign to MNs that are within the specified range. ip_address3 must be specified in either IPv4 dotted decimal notation or IPv6 colon notation.

Usage
Use this command to assign ranges of MN IP addresses to specific HAs.

Important: A maximum of 8 MIP HA assignment tables can be configured per context with a maximum of 8 MIP HA assignment tables across all contexts.

Important: A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

Example
The following command assigns any MN IP address that falls in the range of 192.168.100.0 through 192.168.101.0 to the HA with the IP address of 192.168.200.10:

    hoa-range 192.168.100.0 192.168.101.0 ha 192.168.200.10
Chapter 150
MIPv6HA Service Configuration Mode Commands

The MIPv6 HA Service Configuration Mode is used to create and manage MIPv6 access privileges.

---

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

Configures the sending of subscriber session AAA accounting by the HA service.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
aaa accounting
no aaa accounting
```

**Usage**
Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers.
The chassis is shipped from the factory with the AAA accounting enabled.

**Important:** In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the `aaa accounting subscriber radius` command.

AAA accounting for the HA service can be disabled using the `no` version of the command.

**Example**
The following command disables aaa accounting for the HA service:

```
no aaa accounting
```
**bind**

Designates the address of the MIPv6HA service and specifies the maximum number of subscribers that can access this service over the interface.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bind address IPv6_address [ max-subscribers count ]
no bind address
```

- **address**
  
  Specifies the IPv6 address (address) of the MIPv6HA service. The IPv6 address size is 128 bits. The preferred IPv6 address representation is: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where each x is a hexadecimal digit representing 4 bits.

- **max-subscribers count**
  
  Default: 3000000
  
  Specifies the maximum number of subscribers that can access this service on this interface. **count** can be configured to any integer value between 0 and 3,000,000.
default

Restore default values assigned for specified parameter.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
default { aaa | refresh-advice-option | refresh-interval-percent | reg-lifetime | sequence-number-validate | setup-timeout | simul-bindings | subscriber | timestamp-replay-protection }
```

**default**
Restores the default values assigned for specified parameter.

**aaa**
Restores the aaa setting configured by the aaa command to its default of enabled.

**refresh-advice-option**
Restores the refresh-advice-option setting to its default of disabled.

**refresh-interval-percent**
Restores the refresh-interval-percent setting to its default of 75.

**reg-lifetime**
Restores the Mobile IP session registration lifetime setting configured by the reg-lifetime command to its default: 600 seconds.

**sequence-number-validate**
Restores the sequence-number-validate setting to its default of enabled.

**setup-timeout**
Restores the maximum amount of time allowed for setting up a session to the default: 60 seconds.

**simul-bindings**
Restores the simultaneous bindings setting to its default: 1.

**subscriber**
Configures settings for the default subscriber.

**timestamp-replay-protection**
Restores the timestamp-replay-protection scheme according to RFC 4285.

Usage
After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

**Example**
The following command is used to return the simultaneous bindings setting parameter to it’s default value:

```plaintext
default simul-bindings
```
end

Exits the HA service configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
**exit**

Exits the HA service configuration mode and returns to the context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the context configuration mode.
**refresh-advice-option**

Confirms inclusion of refresh advice option in Binding Acknowledgement sent by Home Agent (HA).

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
refresh-advice-option
```

**Usage**

Includes the refresh advice option in the binding acknowledgements sent by the home agent. Default is disabled.
refresh-interval-percent

Configures percentage of the granted lifetime to be used in the refresh interval mobility option in Binding Acknowledgement sent by Home Agent (HA).

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
refresh-interval-percent value
```

- **value**
  - Value represents a percentage. Default is 75.

**Usage**
Use this command to configure the amount of the granted lifetime to be used in the refresh interval mobility option in Binding Acknowledgement sent by Home Agent (HA).

**Example**
The following command sets the refresh-interval-percent value to 50%:

```
refresh-interval-percent 50
```
**reg-lifetime**

Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
reg-lifetime time

no reg-lifetime
```

- **no**
  Sets the registration lifetime to infinite.

- **time**
  Specifies the registration lifetime.
  time is measured in seconds and can be configured to any integer value between 1 and 262140. Default is 600.

**Usage**

Use to limit a mobile nodes lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply.

The chassis is shipped from the factory with the registration lifetime set to 600 seconds.

**Example**
The following command configures the registration lifetime for the HA service to be 2400 seconds:

```
reg-lifetime 2400
```

The following command configures an infinite registration lifetime for MIPv6 calls:

```
no reg-lifetime
```
sequence-number-validate

Configures sequence number validation of the received MIPv6 control packet by the Home Agent (HA) according to RFC 3775.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

sequence-number-validate

Usage
Use this command to configure the sequence number validation of the received MIPv6 control packet by the Home Agent (HA) as per RFC 3775. Default is enabled.
setup-timeout

The maximum amount of time allowed for session setup.

**Product**

PDSN, HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
setup-timeout seconds
```

- **seconds**
  
  Default: 60 seconds
  
  The maximum amount of time, in seconds, to allow for setup of a session. must be an integer from 1 through 1000000. Default is 60 seconds.

**Usage**

Use this command to set the maximum amount of time allowed for setting up a session.

**Example**

To set the maximum time allowed for setting up a session to 5 minutes (300 seconds), enter the following command:

```
setup-timeout 300
```
simul-bindings

Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
simul-bindings number
```

<table>
<thead>
<tr>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures maximum number of &quot;care of&quot; addresses that can be simultaneously bound for the same user as identified by their NAI and home address. number can be configured to any integer value between 1 and 3. Default is 1.</td>
</tr>
</tbody>
</table>

Usage
The chassis is shipped from the factory with the simultaneous sessions set to 1. Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address. Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintains previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested.

Example
The following command configures the service to support up to 2 addresses per subscriber:

```
simul-bindings 2
```
timestamp-replay-protection tolerance

Designates timestamp replay protection scheme as per RFC 4285.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

timestamp-replay-protection tolerance
tolerance

Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds. tolerance must be an integer between 0 and 65535. The default is 7 seconds.

Usage
Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.
Chapter 151
MME-HSS Service Configuration Mode Commands

The MME-HSS Service Configuration Mode is used to create and manage the HSS servers on Diameter protocol.

```
Exec Mode
  configure
    Global Config Mode
      context name
        Context Config Mode
          mme-hss-service name
            MME HSS Service Config Mode
```
diameter dictionary

Specifies the Diameter Credit Control dictionary for the MME-HSS service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter dictionary { custom1 | standard }
default diameter dictionary

default
Sets the dictionary to default for HSS service.

custom1
Default: Disabled
This keyword sets the Diameter dictionary to customer specific dictionary. This is a customer specific
diameter dictionary.

standard
Default: Enabled
This keyword sets the Diameter dictionary to Standard dictionary. This is standard MME-HSS dictionary.

Usage
Use this command to select the Diameter dictionary for MME-HSS service.

Example
The following command sets the Diameter dictionary to IETF RFC 4006 specific:
diameter dictionary standard
diameter endpoint

This command associates a preconfigured Diameter origin endpoint with this MME-HSS service to manage S6a interface between MME and HSS.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] diameter endpoint <endpoint_name> [-noconfirm]

- no
Removes previously associated Diameter origin endpoint from this MME-HSS service.

- endpoint_name
This is a preconfigured Diameter endpoint in Context configuration mode. The endpoint must be present in all Diameter messages and is the endpoint that originates the Diameter message.
<endpoint_name> must be an preconfigured diameter endpoint name.
If named endpoint is not configured earlier the system will create it and switch to the Diameter Endpoint Configuration mode in Context Configuration mode.

- -noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**WARNING:** If this keyword option is used with no diameter endpoint <endpoint_name> command the Diameter endpoint named <endpoint_name> will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

Use this command to associate a Diameter origin endpoint to create Diameter-based S6a interface in this MME-HSS service to provide AAA functionality to EPS bearer context.
If named endpoint is not configured earlier the system will create it and switch to the Diameter Endpoint Configuration mode in Context Configuration mode.
Refer Diameter Endpoint Configuration Mode Commands chapter for more information on Diameter endpoint configuration parameters.

Example

The following command associates the preconfigured Diameter endpoint hss_1 with this MME-HSS service for S6a interface support.

diameter endpoint hss_1
If named endpoint is not configured earlier the system will create it and switch to the Diameter Endpoint Configuration mode in Context Configuration mode and following prompt will appear:

```
[context]host(config-ctx-diameter)#
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
   end

Usage
   Change the mode back to the Exec mode.
**exit**

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Return to the previous mode.
failure-handling

This command configures the failure handling behavior in the event of a failure with the MME-HSS service. It also defines the action on various error codes on Diameter interface during authentication or session activities.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
failure-handling {authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request} {diameter-result-code start_error_code[to end_error_code] | request-timeout} action {continue | retry-and-terminate | terminate}
```

```
no failure-handling {authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request} diameter-result-code start_error_code[to end_error_code]
```

default failure-handling {authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request} request-timeout

---

**no**
Removes the preconfigured failure handling procedures for MME calls in an MME-HSS service.

---

**default**
Sets the default action for failure handling procedure for MME calls in an MME-HSS service. For default actions on Diameter result/error codes see Usage section of this section.

---

**authentication-information-request**
This keyword configures the MME-HSS service to handle the failures in Auth-Information-Request message.

---

**check-identity-request**
This keyword configures the MME-HSS service to handle the failures in Check-Identity-Information-Request message.

---

**notify-request**
This keyword configures the MME-HSS service to handle the failures in Notify-Request message.

---

**purge-ue-request**
This keyword configures the MME-HSS service to handle the failures in Purge-UE-Request message.

---

**update-location-request**
This keyword configures the MME-HSS service to handle the failures in Update-Location-Request message.
**diameter-result-code start_error_code [to end_error_code]**

This keyword configures the MME-HSS service to handle the failures for various request message having specific single or range of Diameter result code in request message.

*start_error_code* specifies the individual error code on Diameter protocol and must be an integer from 3000 through 5999. This will be the starting of code if a range of error codes is specified with optional keyword *to* *end_error_code*.

*to* *end_error_code* is used to specify a range of error codes to handle by this command.

*end_error_code* specifies the end error code on Diameter protocol and must be an integer from 3000 through 5999.

**request-timeout**

This keyword configures the MME-HSS service to handle the failures for various request messages if response to that message is not received before timeout duration exhausted.

**action {continue | retry-and-terminate | terminate}**

This keyword specifies the action to be taken on failure of any message as policy of failure handling.

- **continue**: On receipt of any error, this action configuration will allow the MME-HSS service to continue with the session procedure without any interruption.

- **retry-and-terminate**: On receipt of any error, this action configuration will instruct the MME-HSS service to retry with the procedure. Sustem will retry up to the configured number of attempts and terminate the session/procedure if it received subsequent number of errors after retry attempts.

- **terminate**: This action configuration will allow the MME-HSS service to terminate the session procedure without any retry attempt on the event of any failure.

**Usage**

Use this command to configure the failure handling behavior in the event of a communication failure with the MME-HSS service.

Following are the default action for Diameter result codes:

- For all protocol error codes 3000 to 3999 the default action is terminate. For all transient error codes 4000, 4001, 4004 to 4180, and 4182 to 4999 the default action is continue.
- For transient error codes 4002, 4003, and 4181 the default action is retry.
- For error code 4001 the default action is terminate.
- For permanent error codes 5000 to 5999 the default action is terminate.

**Example**

The following command will allow MME-HSS service to continue if any failure in Auth-Information-Request message occurred with Diameter error code 3050:

```
failure-handling authentication-information-request diameter-result-code 3050 action continue
```
request timeout

This command configures the application request timeout between MME-HSS service and HSS node. The MME system will wait for this duration before retransmitting the request to corresponding HSS node.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```plaintext
request timeout dur

[ no | default ] request timeout

---

no
Disables the configured application request timeout value.

---

default
Sets the application request time out duration to default value of 300 seconds.

---

dur
Default: 300 seconds
Specifies the application request timeout duration in seconds. The MME will wait for this duration before retrying the request with corresponding HSS.
dur must be an integer from 1 through 300.
```

Usage
Use this command to set the waiting period for MME-HSS service in seconds after which the request is deemed to have failed or system will resend the request.

Example
The following example configures the application request timeout duration to 300 seconds:
```
default request timeout
```
test

This command test the configured S6a interface between MME-HSS service and HSS server.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

test s6a_inf_name
[ no | default ] test

no
Removes the configured S6a test interface from this MME-HSS service.

default
Sets the S6a test interface to default interface configured from MME service.

s6a_inf_name
Specifies the name of the S6a interface which is to be used for testing the connectivity between MME and HSS node.

s6a_inf_name is a preconfigured interface for S6a reference on system and must be an alpha and/or numerical string of 1 through 63 characters.

Usage
Use this command to set the S6a interface for testing between MME and HSS node.

Example
The following command configures S6a test interface to s6a_1:

```
test s6a_1
```
Chapter 152
MME Service Configuration Mode Commands

The MME Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) services for LTE/SAE network. This service works in conjunction with MME-HSS Service and eGTP Service.
apn

This command associates/disassociates an Access Point Name (APN) templates to use in MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
apn
```

```
no apn
```

**no**
Disassociates a previously associated APN template with this MME service.

**apn_name**
Specifies the name for a pre-configured APN template to associate with this MME service.

**-noconfirm**
Indicates that the command is to execute without any additional prompt and confirmation from the user.

**WARNING**: If this keyword option is used with **no apn** command the APN named **apn_name** will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

**Usage**
Use this command to associate a pre-configured APN template with an MME service. The APN is a logical name for a packet data network and/or a service that the SGSN/GGSN supports access to. Multiple APN templates can be associated with an MME service.

**Example**
The following command associates an APN template called *isp1* to an MME service:

```
apn isp1
```
**associate**

This command associates/disassociates the supportive services like an Evolved GPRS Tunnelling Protocol (eGTP) service or an MME-HSS service with an MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
associate { egtp-service egtp_svc_name | mme-hss-service hss_svc_name } [ context ctx_name ]
```

```
no associate { egtp-service | mme-hss-service }
```

**no**
Disassociates a previously associated eGTP service or MME-HSS service with this MME service.

**egtp-service egtp_svc_name**
Associates an eGTP service with MME service.
*egtp_svc_name* specifies the name for a pre-configured eGTP service in a context to associate with this MME service. For more information on eGTP service, refer egtp-service command in Context Configuration Mode Commands chapter.

**mme-hss-service hss_svc_name**
Associates an MME-HSS service with MME service.
*hss_svc_name* specifies the name for a pre-configured MME-HSS service in a context to associate with this MME service. For more information on MME HSS service, refer mme-hss-service command in Context Configuration Mode Commands chapter.

**context ctx_name**
Specifies the specific context name where eGTP or MME-HSS service is configured. If this keyword is omitted, the named eGTP or MME-HSS service must exist in the same context as the MME service.
*ctx_name* is name of the configured context of the eGTP or MME-HSS service service. This can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**Usage**
Use this command to associate a pre-configured eGTP or MME-HSS service with an MME service.
The eGTP service provides eGTP-U and eGTP-C protocol interface support between EPS nodes. For more information on eGTP service and supported interface type, refer eGTP Service Configuration Mode Commands chapter in Command Line Interface Reference.

⚠️ **Important**: Only one eGTP service can be associated to a service. The eGTP service should be configured prior to issuing this command.
The MME-HSS service provides S6a interface support on Diameter protocol between MME and HSS. For more information on MME-HSS service and other parameters, refer MME-HSS Service Configuration Mode Commands chapter in Command Line Interface Reference.

**Important:** Only one MME-HSS service can be associated to a service in this release. The eGTP service should be configured prior to issuing this command.

**Caution:** This is a critical configuration. The MME service can not be started without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.

**Example**
The following command associates a pre-configured eGTP service called egtp1 in dst_ctx context to an MME service:

```
associate egtp-service egtp1 context dst_ctx
```

The following command associates a pre-configured MME-HSS service called hss1 in the same context as MME service to an MME service:

```
associate mme-hss-service hss1
```
bind s1-mme

This command binds the MME service to a logical IP interface serving as the S1-MME interface.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

bind s1-mme address address
no bind address

no
Removes a previously configured IP address use for binding the SCTP (local bind address) to communicate with the eNodeBs using S1-MME interface.

address
Specifies the IP address (address) in IPv4 or IPv6 notation for the interface configured as an S1-MME interface.

Usage
Use this command to associate or tie the MME service to a specific logical IP address that will be used for binding the SCTP socket to communicate with the eNodeB using S1AP. A maximum of one IP address can be configured with this command for one MME service.
The MME passes the IP address during setting up the SCTP association with the eNodeB.

⚠️ Caution: This is a critical configuration. The MME service can not be started without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.

Example
The following command would bind the logical IP interface with the address of 192.168.3.1 to the MME service to interact with eNodeB.

bind s1-mme address 192.168.3.1

The following command disables a binding that was previously configured:

no bind s1-mme address
dns

This command associates/disassociates the Domain Name System (DNS) client service configured for DNS query in a context to select P-GW and S-GW in an MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
dns { pgw | sgw } [ context ctx_name ]
no dns { pgw | sgw }
```

no
Disassociates a previously associated context having DNS client service configured for DNS query to select P-GW or S-GW with this MME service.

pgw
This keyword associates the named context with DNS client service for DNS query for selection of P-GW with MME service.

sgw
This keyword associates the named context with DNS client service for DNS query for selection of S-GW with MME service.

context ctx_name
This optional keyword associates the specific context name where DNS client service is configured to select P-GW and/or S-GW for this MME service. If this keyword is omitted DNS client service must be configured in the same context as MME service.

ctx_name is name of the configured context of the DNS client service. This can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Usage
Use this command to associate a pre-configured context where a DNS client service is configured with an MME service.
The DNS Client service configured in a context provides the DNS query support to locate P-GW or S-GW from and MME service. For more information on DNS Client service and support, refer DNS Client Service Configuration Mode Commands chapter in Command Line Interface Reference.
A maximum of one DNS client service for P-GW and one DNS client service for S-GW can be associated with an MME service.

Example
The following command associates a pre-configured context `dns_ctx1` where a DNS client service is configured for DNS query to P-GW from an MME service:

```
dns pgw context dns_ctx1
```

The following command associates a pre-configured context `dns_ctx2` where a DNS client service is configured for DNS query to S-GW from an MME service:

```
dns sgw context dns_ctx2
```
This command defines the Evolved Mobility Management timer parameters like timeout durations for timers for the NAS message retransmission in MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default emm {mobile-reachable-timeout | t3412-timeout | T3413-timeout | T3422-timeout | T3423-timeout | T3450-timeout | T3460-timeout | T3470-timeout }

no emm implicit-detach-timeout
```

- **default**
  - Resets the specified timer timeout to the system default value.

- **no**
  - Removes the specified EMM timeout definition from the configuration.

- **implicit-detach-timeout**
  - `detach_dur`
  - Default: 5640
  - Sets the timer timeout duration after which subscriber will implicitly detached from the network if there is no activity. Generally this timer value is 240 seconds (4 minutes) more than the timeout value of T3423 timer. This timer starts when mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated and stops when NAS signalling connection established.

- **mobile-reachable-timeout**
  - `mob_reach_dur`
  - Default: 5640
  - Sets the timeout timer duration after which reachability procedure will be discarded and reattempt starts.

- **t3412-timeout**
  - `t3412_dur`
  - Default: 5400
  - Sets the timeout duration for T3412 timer. This timer is used for periodic tracking area update (P-TAU). When this timer expires, the periodic tracking area updating procedure starts and the timer is set to its initial value for the next start. This timer starts when the UE goes from EMM-CONNECTED to EMM-IDLE mode and stops when the UE enters EMM-CONNECTED mode.

- **T3413-timeout**
  - `t3413_dur`
  - Default: 10
Sets the timeout duration for T3413 timer. The timer starts when MME initiates the EPS paging procedure to the EMM entity in the network and requests the lower layer to start paging. This timer stops for the paging procedure when a response received from the UE.

t3413_dur is timeout duration in seconds and must be an integer from 1 through 20.

**T3422-timeout t3422_dur**

Default: 10

Sets the timeout duration for T3422 timer. This timer starts when MME initiates the detach procedure by sending a DETACH REQUEST message to the UE and stops upon receipt of the DETACH ACCEPT message.

t3422_dur is timeout duration in seconds and must be an integer from 1 through 20.

**T3423-timeout t3423_dur**

Default: 5400

Sets the timeout duration for T3423 timer. This timer starts when UE enters the EMM-DEREGISTERED state or when entering EMM-CONNECTED mode. It stops while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE state and Idle mode Signalling Reduction (ISR) is activated.

t3423_dur is timeout duration in seconds and must be an integer from 1 through 11160.

**T3450-timeout t3450_dur**

Default: 6

Sets the timeout duration for T3450 timer. This timer starts when MME initiates the Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and stops upon receipt of the GUTI REALLOCATION COMPLETE message.

This timer is also used for Tracking area update procedure.

t3450_dur is timeout duration in seconds and must be an integer from 1 through 20.

**T3460-timeout t3460_dur**

Default: 6

Sets the timeout duration for T3460 timer. The timers starts when the network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and stops upon receipt of the AUTHENTICATION RESPONSE message.

t3460_dur is timeout duration in seconds and must be an integer from 1 through 20.

**T3470-timeout t3470_dur**

Default: 6

Sets the timeout duration for T3470 timer. The MME starts this timer when the network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and stops upon receipt of the IDENTITY RESPONSE message.

t3470_dur is timeout duration in seconds and must be an integer from 1 through 20.

**Usage**

Use this command to set EMM timers.

Following tables describe the triggers and states for timers:
### Table 28. EPS mobility management timers – UE side

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry</th>
</tr>
</thead>
</table>
| T3402 | • EMM-DEREGISTERED  
       | • EMM-REGISTERED  | • At attach failure and the attempt counter is equal to 5.  
 |       |       | • At tracking area updating failure and the attempt counter is equal to 5.  | • ATTACH REQUEST sent  
       |       |               | • TRACKING AREA UPDATE REQUEST sent  | Initiation of the attach procedure or TAU procedure |
|       | EMM-REGISTERED-INITIATED | ATTACH REQUEST sent | • ATTACH ACCEPT received  
 |       |       |               | • ATTACH REJECT received  | Start T3411 or T3402 as described in subclause 5.5.1.2.6 |
| T3411 | • EMM-DEREGISTERED. ATTEMPTING -TO-ATTACH  
       | • EMM-REGISTERED. ATTEMPTING -TO-UPDATE  | • At attach failure due to lower layer failure, T3410 timeout or attach rejected with other EMM cause values than those treated in subclause 5.5.1.2.5.  
 |       |       | • At tracking area updating failure due to lower layer failure, T3430 timeout or TAU rejected with other EMM cause values than those treated in subclause 5.5.3.2.5.  | • ATTACH REQUEST sent  
       |       |               | • TRACKING AREA UPDATE REQUEST sent  | Retransmission of the ATTACH REQUEST or TRACKING AREA UPDATE REQUEST |
| T3412 | EMM-REGISTERED | In EMM-REGISTERED, when EMM-CONNECTED mode is left.  | • When entering state EMM-DEREGISTERED or  
<p>|       |       |               | • When entering EMM-CONNECTED mode.  | Initiation of the periodic TAU procedure |</p>
<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3416</td>
<td>• EMM-REGISTERED-INITIATED</td>
<td>RAND and RES stored as a result of a UMTS authentication challenge</td>
<td>• SECURITY MODE COMMAND received</td>
<td>Delete the stored RAND and RES</td>
</tr>
<tr>
<td></td>
<td>• EMM-REGISTERED</td>
<td></td>
<td>• SERVICE REJECT received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EMM-DEREGISTERED-INITIATED</td>
<td></td>
<td>• TRACKING AREA UPDATE ACCEPT received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EMM-TRACKING-AREA-UPDATING-INITIATED</td>
<td></td>
<td>• AUTHENTICATION REJECT received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EMM-SERVICE-REQUEST-INITIATED</td>
<td></td>
<td>• AUTHENTICATION FAILURE sent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• EMM-DEREGISTERED or EMM-NUL entered</td>
<td></td>
</tr>
<tr>
<td>T3417</td>
<td>EMM-SERVICE-REQUEST-INITIATED</td>
<td>• SERVICE REQUEST sent</td>
<td>• Bearer have been set up</td>
<td>Abort the procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EXTENDED SERVICE REQUEST sent in case f and g in subclause 5.6.1.1</td>
<td>• SERVICE REJECT received</td>
<td></td>
</tr>
<tr>
<td>T3417ext</td>
<td>EMM-SERVICE-REQUEST-INITIATED</td>
<td>• EXTENDED SERVICE REQUEST sent in case d in subclause 5.6.1.1</td>
<td>• Inter-system change from S1 mode to A/Gb mode or Iu mode is completed</td>
<td>Abort the procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EXTENDED SERVICE REQUEST sent in case e in subclause 5.6.1.1 and the CSFB response was set to “CS fallback accepted by the UE”.</td>
<td>• Inter-system change from S1 mode to A/Gb mode or Iu mode is failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SERVICE REJECT received</td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>State</td>
<td>Cause of Start</td>
<td>Normal Stop</td>
<td>On Expiry</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| T3418 | - EMM-REGISTERED-INITIATED  
- EMM-REGISTERED  
- EMM-TRACKING-AREA-UPDATING-INITIATED  
- EMM-DEREGISTERED-INITIATED  
- EMM-SERVICE-REQUEST-INITIATED | AUTHENTICATION FAILURE (EMM cause = #20 “MAC failure” or #26 “Non-EPS authentication unacceptable”) sent | AUTHENTICATION REQUEST received | On first expiry, the UE should consider the network as false |
| T3420 | - EMM-REGISTERED-INITIATED  
- EMM-REGISTERED  
- EMM-DEREGISTERED-INITIATED  
- EMM-TRACKING-AREA-UPDATING-INITIATED  
- EMM-SERVICE-REQUEST-INITIATED | AUTHENTICATION FAILURE (cause = #21 “synch failure”) sent | AUTHENTICATION REQUEST received | On first expiry, the UE should consider the network as false |
<p>| T3421 | EMM-DEREGISTERED-INITIATED | DETACH REQUEST sent | DETACH ACCEPT received | Retransmission of DETACH REQUEST |</p>
<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3423</td>
<td>EMM-REGISTERED</td>
<td>T3412 expires while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE and ISR is activated.</td>
<td>- When entering state EMM-DEREGISTERED or EMM-CONNECTED mode.</td>
<td>Set TIN to “P-TMSI”</td>
</tr>
<tr>
<td>T3430</td>
<td>EMM-TRACKING-AREA-UPDATING-INITIATED</td>
<td>TRACKING AREA UPDATE REQUEST sent</td>
<td>- TRACKING AREA UPDATE ACCEPT received</td>
<td>Start T3411 or T3402 as described in subclause 5.5.3.2.6</td>
</tr>
<tr>
<td>T3440</td>
<td>- EMM-REGISTERED-INITIATED</td>
<td></td>
<td>- ATTACH REJECT, DETACH REQUEST, TRACKING AREA UPDATE REJECT with any of the EMM cause values #11, #12, #13, #14 or #15</td>
<td>- Signalling connection released</td>
</tr>
<tr>
<td></td>
<td>- EMM-TRACKING-AREA-UPDATING-INITIATED</td>
<td></td>
<td>- SERVICE REJECT received with any of the EMM cause values #11, #12, #13 or #15</td>
<td>- Bearers have been set up</td>
</tr>
<tr>
<td></td>
<td>- EMM-DEREGISTERED-INITIATED</td>
<td></td>
<td>- TRACKING AREA UPDATE ACCEPT received after the UE sent TRACKING AREA UPDATE REQUEST in EMM-IDLE mode with no “active” flag</td>
<td>Release the signalling connection and proceed as described in subclause 5.3.1.2</td>
</tr>
<tr>
<td></td>
<td>- EMM-SERVICE-REQUEST-INITIATED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- EMM-REGISTERED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3442</td>
<td>EMM-REGISTERED</td>
<td>SERVICE REJECT received with EMM cause #39</td>
<td>TRACKING AREA UPDATE REQUEST sent</td>
<td>None</td>
</tr>
</tbody>
</table>

NOTE 1: The default value of this timer is used if the network does not indicate another value in an EMM signalling procedure.

NOTE 2: The value of this timer is provided by the network operator during the attach and tracking area updating procedures.

NOTE 3: The value of this timer may be provided by the network in the ATTACH ACCEPT message and TRACKING AREA UPDATE ACCEPT message. The default value of this timer is identical to the value of T3412.

NOTE 4: The value of this timer is provided by the network operator when a service request for CS fallback is rejected by the network with EMM cause #39 “CS domain temporarily not available”.

Cisco ASR 5000 Series Command Line Interface Reference  | 3853
Table 29. EPS mobility management timers – network side

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3413</td>
<td>EMM-REGISTERED</td>
<td>Paging procedure initiated</td>
<td>Paging procedure completed</td>
<td>Network dependent</td>
</tr>
<tr>
<td>T3422</td>
<td>EMM-DEREGISTERED-INITIATED</td>
<td>DETACH REQUEST sent</td>
<td>DETACH ACCEPT received</td>
<td>Retransmission of DETACH REQUEST</td>
</tr>
<tr>
<td>T3450</td>
<td>EMM-COMMON-PROC-INIT</td>
<td>● ATTACH ACCEPT sent</td>
<td>● ATTACH COMPLETE received</td>
<td>Retransmission of the same message type, i.e. ATTACH ACCEPT, TRACKING AREA UPDATE COMPLETE received</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● TRACKING AREA UPDATE ACCEPT sent with GUTI</td>
<td>● TRACKING AREA UPDATE COMPLETE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>● GUTI REALLOCATION COMMAND sent</td>
<td>● GUTI REALLOCATION COMPLETE received</td>
<td></td>
</tr>
<tr>
<td>T3460</td>
<td>EMM-COMMON-PROC-INIT</td>
<td>● AUTHENTICATION REQUEST sent</td>
<td>● AUTHENTICATION RESPONSE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>● SECURITY MODE COMMAND sent</td>
<td>● AUTHENTICATION FAILURE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● SECURITY MODE COMPLETE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● SECURITY MODE REJECT received</td>
<td></td>
</tr>
<tr>
<td>T3470</td>
<td>EMM-COMMON-PROC-INIT</td>
<td>IDENTITY REQUEST sent</td>
<td>IDENTITY RESPONSE received</td>
<td>Retransmission of IDENTITY REQUEST</td>
</tr>
<tr>
<td>Mobile reachable timer</td>
<td>All except EMM-DEREGISTERED</td>
<td>Entering EMM-IDLE mode</td>
<td>NAS signalling connection established</td>
<td>Network dependent, but typically paging is halted on 1st expiry</td>
</tr>
<tr>
<td>Implicit detach timer</td>
<td>All except EMM-DEREGISTERED</td>
<td>The mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated</td>
<td>NAS signalling connection established</td>
<td>Implicitly detach the UE on 1st expiry</td>
</tr>
</tbody>
</table>

NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

NOTE 2: The value of this timer is network dependent.
### Table 30. EPS session management timers – UE side

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3480</td>
<td>PROCEDURE TRANSACTION PENDING</td>
<td>BEARER RESOURCE ALLOCATION REQUEST sent</td>
<td>ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE ALLOCATION REJECT received</td>
<td>Retransmission of BEARER RESOURCE ALLOCATION REQUEST</td>
</tr>
<tr>
<td>T3481</td>
<td>PROCEDURE TRANSACTION PENDING</td>
<td>BEARER RESOURCE MODIFICATION REQUEST sent</td>
<td>ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or DEACTIVATE EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE MODIFICATION REJECT received</td>
<td>Retransmission of BEARER RESOURCE MODIFICATION REQUEST</td>
</tr>
<tr>
<td>T3482</td>
<td>PROCEDURE TRANSACTION PENDING</td>
<td>An additional PDN connection is requested by the UE which is not combined in attach procedure</td>
<td>ACTIVE DEFAULT EPS BEARER CONTEXT REQUEST received or PDN CONNECTIVITY REJECT received</td>
<td>Retransmission of PDN CONNECTIVITY REQUEST</td>
</tr>
<tr>
<td>T3492</td>
<td>PROCEDURE TRANSACTION PENDING</td>
<td>PDN DISCONNECT REQUEST sent</td>
<td>DEACTIVATE EPS BEARER CONTEXT REQUEST received or PDN DISCONNECT REJECT received</td>
<td>Retransmission of PDN DISCONNECT REQUEST</td>
</tr>
</tbody>
</table>

NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

### Table 31. EPS session management timers – Network side

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>State</td>
<td>Cause of Start</td>
<td>Normal Stop</td>
<td>On Expiry 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>T3485</td>
<td>BEARER CONTEXT ACTIVE PENDING</td>
<td>- ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent</td>
<td>- ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent</td>
<td>Retransmission of the same message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3486</td>
<td>BEARER CONTEXT MODIFY PENDING</td>
<td>MODIFY EPS BEARER CONTEXT REQUEST sent</td>
<td>- MODIFY EPS BEARER CONTEXT ACCEPT received or</td>
<td>Retransmission of MODIFY EPS BEARER CONTEXT REQUEST</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- MODIFY EPS BEARER CONTEXT REJECT received</td>
<td></td>
</tr>
<tr>
<td>T3489</td>
<td>PROCEDURE TRANSACTION PENDING</td>
<td>ESM INFORMATION REQUEST sent</td>
<td>ESM INFORMATION RESPONSE received</td>
<td>Retransmission of ESM INFORMATION REQUEST on 1st and 2nd expiry only</td>
</tr>
<tr>
<td>T3495</td>
<td>BEARER CONTEXT INACTIVE PENDING</td>
<td>DEACTIVATE EPS BEARER CONTEXT REQUEST sent</td>
<td>DEACTIVATE EPS BEARER CONTEXT ACCEPT received</td>
<td>Retransmission of DEACTIVATE EPS BEARER CONTEXT REQUEST</td>
</tr>
</tbody>
</table>

NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

This command can be repeated to set each timer as needed. The retransmission of all type of NAS messages can be configured through `nas-max-retransmissions` command.

Example
The following command sets the timeout value for EPS paging procedure timer T3413 for 10 seconds.

```
emmm t3413-timeout 10
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
encryption-algorithm-lte

This command configures the precedence for LTE encryption algorithms to use for security procedures through this MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**
```
encryption-algorithm-lte priority1 {128-eea0 | 128-eea1 | 128-eea2}
[priority2 {128-eea0 | 128-eea1 | 128-eea2}] [priority3 {128-eea0 | 128-eea1 | 128-eea2}]
default encryption-algorithm-lte
```

**default**
Sets the default LTE encryption algorithm for security procedures with configured priority value. Default configuration of LTE encryption algorithm is:
- priority1 with 128-eea0 encryption algorithm
- priority2 with 128-eea1 encryption algorithm
- priority3 with 128-eea2 encryption algorithm

**priority1**
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1. Least value has highest preference.

**priority2**
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2. Least value has highest preference.

**priority3**
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 3. Least value has highest preference.

**128-eea0**
Default: Enabled
This keyword sets the Null ciphering algorithm (128-EAA0) for LTE encryption as the encryption algorithm for security procedures.

**128-eea1**
Default: Disabled
This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EAA1) for LTE encryption as the encryption algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2.
**128-eea2**

Default: Disabled
This keyword sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.

**Usage**

Use this command to set the LTE encryption algorithms for security procedures to use with this MME service.

⚠️ **Caution:** When this command is executed, all the existing priority to algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

⚠️ **Caution:** Configuration of same algorithm to multiple priorities is prohibited.

**Example**
The following command sets the 128-EEA1 as the LTE encryption algorithm with priority 2 for security procedures with an MME service.

```
encryption-algorithm-lte priority2 128-eea1
```
esm

This command defines the Evolved Session Management timer parameters like timeout durations for timers for the retransmission of NAS messages in MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

default esm {t3485-timeout|T3495-timeout}

default
Resets the specified Evolved Session Management timer timeout to the system default value.

t3485-timeout \textit{t3485\_dur}
Default: 6
Sets the timeout duration for T3485 timer. This timer is used for default EPS bearer context activation procedure.
This timer starts when the MME sends ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to UE and stops when receives ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT or ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message from UE.
\textit{t3485\_dur} is timeout duration in seconds and must be an integer from 1 through 60.

T3495-timeout \textit{t3495\_dur}
Default: 6
Sets the timeout duration for T3485 timer. This timer is used for default EPS bearer context deactivation procedure.
This timer starts when the MME sends DEACTIVATE EPS BEARER CONTEXT REQUEST message to UE and stops when receives DEACTIVATE EPS BEARER CONTEXT ACCEPT or DEACTIVATE EPS BEARER CONTEXT REJECT message from UE.
\textit{t3495\_dur} is timeout duration in seconds and must be an integer from 1 through 60.

Usage
Use this command to set Evolved Session Management timers.
Following tables describe the triggers and states for timers:

\textit{Table 32. EPS session management timers – Network side}

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer</td>
<td>State</td>
<td>Cause of Start</td>
<td>Normal Stop</td>
<td>On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
<td>---------------------------------------------</td>
</tr>
</tbody>
</table>
| T3485 | Bearer Context Active Pending | • ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent  
• ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST sent | • ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT received or  
• ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT received | Retransmission of the same message |
| T3495 | Bearer Context Inactive Pending | DEACTIVATE EPS BEARER CONTEXT REQUEST sent | DEACTIVATE EPS BEARER CONTEXT ACCEPT received | Retransmission of DEACTIVATE EPS BEARER CONTEXT REQUEST |

NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

This command can be repeated to set each timer as needed. The retransmission of all type of NAS messages can be configured through `nas-max-retransmissions` command.

**Example**
The following command sets the timeout value for default EPS bearer context activation procedure timer T3485 for 10 seconds.

```
esm t3485-timeout 10
```
**exit**

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the previous mode.
**imei**

This command sets the mobile equipment identity (MEI) query criteria with different attributes like IMEI and IMEI-SV for UE related procedures.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
imei-query-type {none | imei | imei-sv}
default imei-query-type
```

- **default**
  
  Sets the UE query criteria to its default type of “none”.

- **imei**
  
  This keyword sets the MEI query type to IMEI. International Mobile Equipment Identity (IMEI) will be used as criteria for MEI query with this MME service.

- **imei-sv**
  
  This keyword sets the MEI query type to IMEI-SV. International Mobile Equipment Identity (IMEI) and software version (SV) will be used as criteria for MEI query with this MME service.

- **none**
  
  This keyword sets the MEI query type to “none”. Neither IMEI nor IMEI-SV will be used as criteria for MEI query with this MME service.

**Usage**

Use this command to MEI query criteria for UE related procedures with an MME service. MME has to do following procedure with reference to MEI query:

- Retrieve MEI from UE during security mode procedure
- Store in local IMSI DB
- Send MEI to HSS in ULR
- Send MEI to SGW in Create Session Request
- Monitor subscriber support using MEI as a key

Query type described with this command will be applicable for all above mentioned procedures.

**Example**

The following command sets the MEI query type to IMEI for UE related procedures:

```
imei-query-type imei
```
integrity-algorithm-lte

This command configures the precedence of LTE integrity algorithms to use for security procedures through this MME service. By default integrity algorithm is enabled on MME service, which cannot be disabled.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

**default integrity-algorithm-lte**

default
Removes the preconfigured integrity algorithm and sets the default LTE integrity algorithm for security procedures. Default configuration of LTE integrity algorithm is:
- priority1 with 128-eia1 integrity algorithm
- priority2 with 128-eia2 integrity algorithm

priority1
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1. This is the mandatory and default priority keyword.

priority2
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

128-eia1
Default: Disabled
This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2.

128-eia2
Default: Enabled
This keyword sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures.

Usage

Use this command to set the LTE integrity algorithms for security procedures to use with this MME service.

⚠️ **WARNING:** Integrity algorithm is a mandatory aspect and can not be disabled in MME service.

⚠️ **Caution:** When this command is executed, all the existing priority to algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.
Caution: Configuration of same algorithm to multiple priorities is prohibited.

Example
The following command sets the AES ciphering algorithms (128-EIA2) as the LTE integrity algorithm with priority as 1 for security procedures with an MME service.

```
integrity-algorithm-lte priority1 128-eia2
```
location-reporting

This command enables the location reporting functionality for UE on MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

[no | default] location-reporting

- default
  Disables the location reporting feature on MME service.

- no
  Disables the location reporting feature on MME service.

Usage
Use this command to enable/disable the UE location reporting feature on MME service.

Example
The following command sets the MME service to provide the location reporting functionality for UE:

location-reporting
max-bearers per-subscriber

This command specifies the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax
```
max-bearers per-subscriber max_bearer
default max-bearers per-subscriber
```

- **default**
  Configures the maximum EPS bearers for a subscriber to use simultaneously to default value of 11.

- **max_bearer**
  Default: 11
  Specifies the maximum number of EPS bearers for a subscriber may simultaneously use to access this MME service.
  `max_bearer` can be configured to any integer value between 1 and 11.

Usage
Use this command to set the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Example
The following command specifies that a maximum of 6 simultaneous EPS bearers can be facilitated for a subscriber at any given time.
```
max-bearers per-subscriber 6
```
max-paging-attempts

This command configures the maximum number of paging attempt retransmission allowed for network requested service creation to a subscriber while first attempt failed.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
max-paging-attempts max_paging_retry
default max-paging-attempts
```

default

Configures the maximum number of retransmission of paging request to default value of 3.

```
max_paging_retry
```

Default: 3

Specifies the maximum number of paging attempt retransmission allowed for network requested service creation to a subscriber while first attempt failed.

```
max_paging_retry
```
can be configured to any integer value between 1 and 10.

Usage

Use this command to set the maximum number of paging attempt retransmission allowed for network requested service creation to a subscriber while first attempt failed.

Example

The following command specifies that a maximum of 6 paging attempt retransmission allowed for network requested service creation to a subscriber while first attempt failed for a subscriber at any given time.

```
max-paging-attempt 6
```
max-pdns per-subscriber

This command specifies the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
max-pdns per-subscriber max_pdns
default max-pdns per-subscriber
```

```
default
Confirms the maximum PDNs for a subscriber simultaneously access through this MME service to default value of 3 PDNs.
```

```
max_pdns
Default: 3
Specifies the maximum number of PDNs that a subscriber may simultaneously access through this MME service.
```

```
max_pdns can be configured to any integer value between 1 and 11.
```

Usage

Use this command to set the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

Example

The following command specifies that a maximum of 2 simultaneous PDNs can be accessed by a subscriber at any given time through this MME service.

```
max-pdns per-subscriber 6
```
mme-id

This command configures the MME identifier with an MME service. MME identifier is constructed with MME group ID and MME Code.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
no mme-id
```

```
mme-id group-id grp_idmme-code mme_code
```

Caution: Removing the MME identifier is a disruptive operation; the MME service shall be removed from the service.

```
  group-id grp_id
```

Specifies the group identifier of for the group of which this MME is belongs to.

`grp_id` must be an integer value from 0 through 65535.

```
mme-code mme_code
```

Specifies the unique code for this MME service.

`mme_code` must be an integer value from 0 through 255.

Usage

Use this command to set the MME identifier for this MME service. This MME identifier will be the identity of this MME in network.

Caution: Changing or removing the MME identifier is a disruptive operation; the MME service shall be re-started or removed from service.

Example

The following command configures the MME identifier with group id as 1025 and MME code as 101 for this MME service.

```
mme-id group-id 1025 mme-code 101
```
nas-max-retransmission

This command sets the retransmission counter for all type of NAS messages in an MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
nas-max-retransmissions nas_retrans_count

default nas-max-retransmissions
```

**default**
Resets the retransmission counter to the system default value of 4.

```
nas_retrans_count
```
Default: 4
Sets the maximum number of retransmission of NAS messages permitted during any procedure after which activation procedure will be discarded.

`nas_retrans_count` is number of retransmission allowed and must be an integer from 1 through 10.

Usage
Use this command to set maximum number of retries allowed for any type of NAS messages. NAS Messages send by the MME which require a response from the UE for procedure completion are retransmitted. Retransmission happens based on timer expiry. The timers are configured through `emm` and `esm` command. The NAS messages are retransmitted as per configuration, and if no response from the UE is received, the pending transaction is abandoned. If the transaction is a DETACH or PDN DISCONNECT REQUEST, the transaction is completed without further UE signaling. The timeout duration configured through `emm` and `esm` command will be applicable between two retries.

Example
The following command sets the maximum number of retries allowed as 4 for all type of NAS messages in an MME service.

```
default nas-max-retransmissions
```
**nri**

This command specifies the Network Resource Identifier (NRI) stored in bit 17 to bit 23 of Globally Unique Temporary Identity (GUTI) to be retrieved by MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nri length length [ value value]
no nri [ value ]
```

**no**
Removes the configured NRI value and location in GUTI for retrieval by this MME service.

**length length**
Specifies the length of bits to be used in the GUTI to retrieve NRI information. This starts from bit 23 to bit 17 of GUTI.

*length* must be an integer from 1 to 6.

**value value**
Specifies the value of NRI to retrieve from GUTI. This value should not exceed the maximum possible value for the specified bit length. For example, if length specified is 3 bit the value should not exceed 7 and if length specified is 5 the value should not exceed 31.

*value* must be an integer from 0 to 63.

**Usage**

Use this command to retrieve the NRI stored in GUTI bit 17 to bit 23.

**Example**
The following command specifies the length of NRI information as 5 bit and value to retrieve as 23 from GUTI:

```
nri length 5 value 23
```
pgw-address

This command configures the PDN Gateway (P-GW) address to use P-MIP protocol for S5 and S8 interface and other parameters with MME service. By default S5 and S8 use GTP protocol for this.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
pgw-address address [ s5-s8-protocol pmip] [ weight value]
no pgw-address address [ s5-s8-protocol pmip ]
```

**no**
Removes a previously configured IP address of P-GW along with S5 and S8 interface of P-MIP protocol type and other parameters from this MME service.

**address**
Specifies the IP address of the P-GW.
*address* must be an IP address in IPv4 or IPv6 notation.

**s5-s8-protocol pmip**
Specifies that P-MIP type of protocol to use for S5 and S8 interfaces with P-GW. By default S5 and S8 interface uses GTP protocol.
*pmip* Sets the protocol to Proxy-MIP for S5 and S8 interface as by default GTP is the applicable protocol.

**weight value**
Assigns the weight to P-GW address to use as a preferred P-GW.
*value* must be an integer from 1 through 100. Lowest value has the least preference.

**Usage**
Use this command to configure the PDN Gateway (P-GW) addresses to use with MME service. This command also changes the default protocol or GTP to P-MIP for the S5 and S8 interface and weight to share the load between associated P-GWs. A maximum of 16 P-GW addresses can be configured with this command.

This command only changes the use of protocol in S5 and S8 interface. By default P-GW uses GTP protocol for S5 and S8 interfaces. By this command user can change the protocol to P-MIP for S5 and S8 interface. When weight is used, the weights of the P-GW(s) (that are operational) are totaled and then weighted round-robin selection is used to distribute new default bearer context among the P-GW(s) according to their weights.

**Example**
The following command associates the P-GW IP address of 192.168.3.1 to the MME service with S5 and S8 protocol as P-MIP and weight as 90.
```
pgw-address 192.168.3.1 s5-s8-protocol pmip weight 90
```
The following command removes the above configured P-GW IP address and other parameters:

```
no pgw-address 192.168.3.15-s8-protocol pmip
```
plmn-id

This command configures the Public Land Mobile Network (PLMN) identifier for this MME service. PLMN identifier is made of Mobile Country Code (MCC) and Mobile Network Code (MNC). A maximum of 16 PLMN id can be configured in an MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
plmn-id mcc mcc_value mnc mnc_value
no plmn-id mcc mcc_value mnc mnc_value
```

no
Removes the configured PLMN identifier for this MME service.

⚠️ **Caution:** Removing the PLMN identifier is a disruptive operation; the MME service shall be re-started.

```
mcc mcc_value
```
Specifies the mobile country code (MCC) part of PLMN identifier.

*mcc_value* must be an integer value from 101 through 998.

```
mnc mnc_value
```
Specifies the mobile network code (MNC) part of PLMN identifier.

*mnc_value* must be an integer value from 01 through 99 or 100 through 998.

**Usage**

Use this command to set the PLMN identifier for this MME service.

⚠️ **Caution:** Changing or removing the PLMN identifier is a disruptive operation; the MME service shall be re-started.

A maximum of 16 PLMN identifiers are supported for an MME service.

**Example**
The following command configures the PLMN identifier with MCC value as 102 and MNC value as 20 for this MME service.

```
plmn-id mcc 102 mnc 20
```
policy idle-mode

This command configures the user-defined policies of session management for LTE subscriber in an MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
policy idle-mode detach {explicit | implicit}
```

```
[default] policy idle-mode detach
```

`default`
Sets the policy of idle mode detach for a subscriber to its default behavior as implicit.

`idle-mode detach`
This keyword configures the IDLE mode detach behavior of a UE.

`detach`
This keyword defines the detach procedure while UE is in IDLE mode.

`explicit`
Default: disabled
This keyword enables the explicit detach while a UE is in IDLE mode. System will page UE before detach procedure started and then perform explicit detach procedure.

`implicit`
Default: Enabled
This keyword enables the implicit detach while a UE is in IDLE mode. System never send any message to UE before detach and performs explicit detach procedure immediately.

Usage
Use this command to set the user-defined policies for session management in this MME service.

Example
The following command sets the idle mode detach policy to explicit for a user in this MME service.

```
policy idle-mode detach explicit
```
policy overload

This command configures the traffic overload policy to control congestion in this service.

**Product**
MME

**Privilege**
Administrator

**Syntax**

cache overload { drop | reject }
default policy overload

default
Sets the traffic overload policy action to default behavior of reject.

drop
Default: Disabled
Specifies that the system is to drop the incoming packets with new session requests to avoid overload on MME node.

reject
Default: Enabled
This keyword configures the system to reject the new session/call request and responds with a reject message when threshold for allowed call session is crossed on MME node.

**Usage**
Use this command to set the user-defined policies for new call connection attempted during overload in an MME service.
Congestion policies at the service-level can be configured for service. When congestion control functionality is enabled at service level, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

**Example**
The following command sets the nw call connect policy to reject the new session/call request in an MME service.
policy overload reject
policy pdn-reconnection

This command configures the action by MME when a PDN connection request to an already connected APN is being processed by MME service.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

policy pdn-reconnection {multiple | reject | restart}

[default] policy pdn-reconnection

default
Sets the policy of PDN reconnection to its default behavior of reject.

multiple
Default: Disabled
This keyword allows multiple connections to a PDN with same APN and PDN Type. In this case, the existing connection is left unchanged, and the MME attempts to establish an additional connection to the PDN.

reject
Default: Enabled
This keyword configures set the action of MME to deny or reject the request, by sending a PDN connection reject command. This is the default behavior.

restart
Default: Disabled
This keyword deletes the existing connection and initiate an attempt to establish a new connection.

Usage
Use this command to set the user-defined policies for PDN reconnection attempt procedures initiated by UE in an MME service.
While a UE is attached, the UE can request connections to PDNs. The PDNs are identified by APN (Access Point Name) and PDN Type (ipv4, ipv6 or ipv4v6).
If the UE requests connection to a PDN for which a connection with the same APN name and PDN type already exists, the MME can; 1) deny or Reject the request, by sending a PDN connection reject command; 2) allow multiple connections to a PDN with same APN and PDN Type; or 3) delete the existing connection, and attempt to establish a new connection.

Example
The following command sets the PDN reconnect policy to delete the existing PDN and start the attempt to establish a new connection in an MME service.

policy pdn-reconnection restart
s1-mme sctp port

This command configures the source SCTP port that will be used for binding the SCTP socket to communicate with the eNodeB using S1AP with this MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
s1-mme sctp port port_num
default s1-mme sctp port
```

**default**
Sets the SCTP port to default value of 699 to communicate with the eNodeBs using S1-MME interface.

**port_num**
Specifies the SCTP port number to communicate with the eNodeBs using S1-MME interface. `port_num` must be an integer between 1 through 65535.

**Usage**
Use this command to assign the SCTP port with SCTP socket to communicate with the eNodeB using S1AP. A maximum of one SCTP port can be associated with one MME service.

**Example**
The following command sets the default SCTP port number 699 for to interact with eNodeB using S1AP on S1-MME interface.

```
default s1-mme sctp port
```
**setup-timeout**

This command configures the timeout duration for call setup of MME calls in this MME service.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
setup-timeout dur
default setup-timeout
```

---

default

Sets the call setup timeout duration to default value of 60 seconds.

---

dur

Default: 60

Specifies the call setup timeout duration for MME calls after which attempt will be discarded.

dur must be an integer between 1 through 10000.

---

**Usage**

Use this command to configured the timeout duration in seconds to setup an MME call with an MME service. One this duration exhausted Call setup procedure will be discarded with this MME service.

---

**Example**

The following command sets the default setup timeout duration of 60 seconds for MME calls:

```
default setup-timeout
```
sgw-address

This command configures the Serving Gateway (S-GW) address to use P-MIP protocol for S5 and S8 interface and other parameters with MME service. By default S5 and S8 use GTP protocol for this.

Product
MME

Privilege
Security Administrator, Administrator

Syntax

```
sgw-address address [ s5-s8-protocol pmip ] [ tai tac tac_value [ mcc mcc_value mnc mnc_value ] [ weight weight_value ]
no sgw-address address [ s5-s8-protocol pmip ] [ tai tac tac_value [ mcc mcc_value mnc mnc_value ] ]
```

**no**
Removes a previously configured IP address of S-GW along with S5 and S8 interface of P-MIP protocol type and other parameters from this MME service.

**address**
Specifies the IP address of the S-GW.
`address` must be an IP address in IPv4 or IPv6 notation.

**s5-s8-protocol pmip**
Specifies that P-MIP type of protocol to use for S5 and S8 interfaces with P-GW. By default S5 and S8 interface uses GTP protocol.
`pmip` Sets the protocol to Proxy-MIP for S5 and S8 interface as by default GTP is the applicable protocol.

**tai tac tac_value**
Specifies the tracking area identifier (TAI) for S-GW. It configures the Tracking Area Code (TAC) for S-GW in MME service.
`tac_value` must be an integer from 1 through 268435455.

**mcc mcc_value**
Specifies the mobile country code (MCC) part of tracking area identifier.
`mcc_value` must be an integer value from 101 through 998.

**mnc mnc_value**
Specifies the mobile network code (MNC) part of tracking area identifier.
`mnc_value` must be an integer value from 01 through 998.

**weight weight_value**
Assigns the weight to P-GW address to use as a preferred S-GW.
`weight_value` must be an integer from 1 through 100. Lowest value has the least preference.
Usage

Use this command to configure the Serving Gateway (S-GW) addresses to use with MME service along with tracking area Identifier and tracking area code. This command also configures the S5 and S8 interface protocol type and priority and weight to share the load between associated S-GWs. A maximum of 16 S-GW addresses can be configured with this command.

This command only changes the use of protocol in S5 and S8 interface. By default S-GW uses GTP protocol for S5 and S8 interfaces. By this command user can change the protocol to P-MIP for S5 and S8 interface. When weight is used, the weights of the S-GW(s) (that are operational) are totaled and then weighted round-robin selection is used to distribute new default bearer context among the S-GW(s) according to their weights.

Example

The following command associates the S-GW IP address of 192.168.3.1 to the MME service with S5 and S8 protocol as P-MIP along with tracking area code as 20 and weight as 90:

```
pgw-address 192.168.3.1 s5-s8-protocol pmip tai tac 20 weight 90
```

The following command removes the above configured S-GW IP address, P-MIP protocol setting, and other parameters:

```
no sgw-address 192.168.3.1 s5-s8-protocol pmip tai tac 20
```
**ue-db**

This command configures the UE database which is maintained by MME as cache of EPS context per UE keyed by IMSI/GUTI to allow UE to attach by GUTI and reuse previously established security parameters. This cache will be maintained in each session manager where the first attach occurred for an UE.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ue-db purge-timeout dur_mins
default ue-db purge-timeout
```

- **default**
  Resets the UE database purge timer timeout to the system default value of 10080 mins.

- **purge-timeout dur_mins**
  Default: 10080
  Sets the timeout duration for MME to store UE database in cache memory.
  This timer starts when UE goes in dormant.
  `dur_mins` is timeout duration in minutes and must be an integer from 1 through 20160.

**Usage**

Use this command to set timeout duration for MME to hold UE database information in cache memory. The MME DB acts as a cache for storing subscriber related information. This subscriber related information helps in reducing signaling traffic. The MME DB is a part of the Session Manager and interfaces between the Session Manager Application and Evolved Mobility Management Manager to provide access to the cached data.

**Example**

The following command configures the MME database cache timer to hold the UE information up to 7 days (10080 minutes) in MME Database.

```
default ue-db purge-timeout
```
Chapter 153
Network Service Entity - Peer NSEI Configuration Mode Commands

The Network Service Entity (NSE) - Peer NSEI configuration mode configures the Frame Relay parameters for the peer NSE. This mode is a sub-mode of the Global Configuration mode. This sub-mode provides the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS Frame Relay network connection.

Upon accessing this mode, the prompt should be similar to:

```
[local]as5000(nse-fr-peer-nsei-2344)#
```

where the 2344 represents a user-defined instance.

---

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

This command has been deprecated.
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

dend

Usage

Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the global configuration mode.
**NS-VC**

This command creates a network service virtual circuit (NSVC) for this frame relay NSE and enters the configuration sub-mode to define the NSVC parameters. These parameters are described in the NSVC Configuration Mode chapter elsewhere in this CLI Reference Guide.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] ns-vc id ns-vc_id
```

- **no**
  Removes the specified NSVC configuration.

- **id ns-vc_id**
  This keyword defines the NSVC configuration identifier.
  *ns-vc_id*: Must be an integer from 0 to 65535

**Usage**

Access the NSVC configuration mode.

**Example**

Gain access to the NSVC configuration mode to change the 4th instance.

```
ns-vc id 4
```
Chapter 154
Network Service Entity- IP Local Configuration Mode Commands

The Network Service Entity (NSE) - IP Local configuration mode is a sub-mode of the Global Configuration mode. This sub-mode configures the local endpoint for NS/IP with the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS IP network connection.

Upon entering this mode, the prompt will appear in a manner similar to:

[local]asr5000(nse-ip-local)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
all-nsvc-failure-action

Configure how the SGSN handles the NSE when all NSVCs go down.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
all-nsvc-failure-action clear-nse
default all-nsvc-failure-action

default
By default, the NSE is not cleared if all NSVCs go down.

clear-nse
Instructs the SGSN to clear NSE if all NSVCs to the BSC are down.
```

**Usage**

Enable the SGSN to clear NSE information when all NSVCs go down.

**Example**

```plaintext
all-nsvc-failure-action clear-nse
```
bssgp-timer

This command has been deprecated.
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Returns to the global configuration mode.
max-ns-retransmissions

This command configures the maximum number of transmission retries counter.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
[ default ] max-ns-retransmissions { alive count | sns-proc count }
```

- **default**
  Resets the specified counter configuration to the default value.

- **alive count**
  Sets the maximum number of alive retries.
  `count`: Must be an integer between 0 and 10. Default is 3.

- **sns-proc count**
  Sets the maximum number of retries for the SNS procedure
  `count`: Must be an integer between 0 and 5. Default is 3.

Usage
Sets the maximum for NS transmission retries.

Example

```
max-ns-retransmission alive 4
```
ns-timer

This command sets the network service (NS) counters for the SNS procedure and testing.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

\texttt{ns-timer \{sns-prov timeout\_val|\ test timeout\_val\}}

default ns-timer \{sns-prov | test\}

\underline{default}

Resets the selected timer configuration to its default value.

\underline{sns-prov timeout\_val}

Sets the SNS procedure timeout value in seconds.
\textit{timeout\_val}: Enter an integer from 1 to 10. Default is 5.

\underline{test timeout\_val}

Sets the test procedure timeout value in seconds.
\textit{timeout\_val}: Enter an integer from 1 to 60. Default is 30 seconds.

Usage

Set NS timers to help manage the NSE-IP connection.

Example

The following example sets the test timer to 4 seconds:

\begin{verbatim}
ns-timer test 4
\end{verbatim}
nsvc-failure-action

This command enables and disables the sending of an NS-STATUS message with cause ‘ip-test fail’ when NSVC goes down.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
nsvc-failure-action send-ns-status
```

```
default nsvc-failure-action
```

**default**
Resets the command configuration to its default value. The default action is not to send an NS-STATUS message. This is applicable only to NSVCs that are auto-learned and not configured.

**send-ns-status**
Enables the sending of the NS-STATUS message.

**Usage**
Use this command to enable or disable sending an NS-STATUS messages when an NSVC goes down.

**Example**
Enable sending of the message:

```
nsvc-failure-action send-ns-status
```
nsvl

This command creates and instance of a Network Service Virtual Link (NSVL) and enters the NSVL configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] nsvl instance nsvl_id

no

Removes the identified NSVL definition from the configuration.

nsvl_id

Identifies a specific NSVL configuration instance.

nsvl_id: Must be an integer from 0 to 3.

Usage

Access the NSVL configuration mode.

Example

nsvl instance 2
peer-network-service-entity

This command has been replaced by the Network Service Entity - Peer NSEI Frame Relay configuration mode.
retry-count

This command has been replaced by the `max-ns-retransmissions` command.
timer

This command has been replaced by the `ns-timer` command.
Chapter 155
Network Service Virtual Connection Configuration Mode Commands

The Network Service Virtual Connection (NSVC) configuration mode is a sub-mode of the Network Service Entity (NSE) - Frame Relay Peer NSEI (NSE-FR for short) configuration mode. This sub-mode provides the commands and parameters to define the management functionality for a specific NSVC of the Gb interface between a BSS and an SGSN in a 2.5G GPRS frame relay network connection.

Upon accessing this mode, the prompt will appear similar to:

[local]asr5000(nse-fr-peer-nsei-2344-nsvci-2)# where the numerics are user-defined ids for the configuration instances.

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

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Return to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the network service entity - frame relay configuration mode.
Chapter 156
Network Service Virtual Link Configuration Mode Commands

The Network Service Virtual Link configuration mode is a sub-mode of the Network Service Entity - IP configuration mode. This sub-mode provides the commands and parameters to define the NSVL of the Gb interface between a BSS and an SGSN in a 2.5G GPRS IP network connection.

Upon entering this mode, the prompt should appear similarly to the following:
[local]asr5000(nse-ip-local-nsvl-1)#

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Returns to the Exec mode.
**exit**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the network service entity - IP configuration mode.
nsvl-address

This command configures the IP address of the NSVL end-point.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

nsvl-address ip-address ip_address context ctxt_name port port_num

<table>
<thead>
<tr>
<th>ip-address  ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the address of the NSVL.</td>
</tr>
<tr>
<td>ip_address: Must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>context  ctxt_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the specific context associated with this NSVL address.</td>
</tr>
<tr>
<td>ctxt_name: Enter up to 79 alphanumeric characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>port  port_num</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the UDP port to associate with the NSVL end-point.</td>
</tr>
<tr>
<td>port_num: Must be an integer from 1 to 65535.</td>
</tr>
</tbody>
</table>

Usage
Use this command to configure the IP address, context name and port number for the NSVL end-point.

Example

nsvl-address ip-address 1.1.1.1 context sgsn2 port 3735
weight

This command configures the signaling or data weight for NSVL.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
weight { data data_weight | signaling signaling_weight }

<table>
<thead>
<tr>
<th>data data_weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the data weight for the NSVL.</td>
</tr>
<tr>
<td>data_weight: Must be an integer from 0 to 255. Default is 1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>signaling signaling_weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the signaling weight for the NSVL.</td>
</tr>
<tr>
<td>signaling_weight: Must be an integer from 0 to 255. Default is 1.</td>
</tr>
</tbody>
</table>

Usage
Configure the weight of the signaling or data for the NSVL.

Example
weight data 234
Chapter 157
NTP Configuration Mode Commands

The Network Timing Protocol Configuration Mode is used to manage the NTP options for the entire system.
enable

Enables the use of the network timing protocol for updating the system clock.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
enable [context]
```

*context*
Default: local
Specifies the context for which NTP is to be enabled. *name* must refer to a previously configured context.

**Usage**
Set the NTP server to be used for the system. Only one NTP server may be active at any given time. If this command were issued in a different context followed by the current context, the prior context’s NTP server would be disabled and the current context’s NTP server would be used.
If any NTP server is enabled, the chassis system clock will be synchronized to the active NTP server which covers all contexts for timing synchronization.
The use of a given context for NTP server assignment is to inherit the domain and IP routing options of the configured context.

**Example**
```
enable sampleContext
```
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```
exit

Exits the NTP configuration mode and returns to the global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the global configuration mode.
**server**

Configures an NTP server for use by the local NTP client in synchronizing the system clock.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
server ip_address[prefer][version number][minpoll poll_period][maxpoll poll_period]
no server ip_address
```

- **no**
  Indicates the server specified is to be removed from the list of NTP servers for clock synchronization.

- **ip_address**
  Specifies the IP address of the NTP server to allow for clock synchronization. *ip_address* must be specified using the standard IPv4 dotted decimal notation.

- **prefer**
  Indicates the NTP server specified to be the preferred server. Only one server can be set to preferred. The preferred server is first contacted for clock synchronization.

**Important:** Use of the prefer keyword is not recommended.

- **version number**
  Default: 4
  Specifies the network timing protocol version to use for server communications. *number* must be a value in the range from 1 to 4.

- **minpoll poll_period**
  Default: 6
  Specifies the minimum polling interval for NTP messages, in seconds, as a power of 2. *poll_period* is the power or exponent. For example, if you specify the number 10, the value is $2^{10}$ and the resultant poll period is 1024 seconds. *poll_period* must be an integer from 6 through 17.

- **maxpoll poll_period**
  Default: 10
  Specifies the maximum polling interval for NTP messages, in seconds, as a power of 2. *poll_period* is the power or exponent. For example, if you specify the number 10, the value is $2^{10}$ and the resultant poll period is 1024 seconds. *poll_period* must be an integer from 6 through 17.
Configure the network timing protocol servers in the network as changes occur.

**Important:** Adding, removing, or modifying an NTP server configuration entry causes the NTP client to restart and restart the synchronization process with all configured NTP servers.

**Example**
The following command adds the NTP server with address 1.2.3.4 to the list of NTP servers.

```
server 1.2.3.4
```

The following marks the server with IP address 1.2.3.4 as the preferred NTP server.

```
server 1.2.3.4 prefer
```
The ORB Element Manager Configuration Mode is used to manage the ORBEM server options for the current context.
activate

Activates/deactivates a client for the ORB element management system interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
activate client id
no activate client id

id name
```

Indicates the client specified is to be deactivated. When omitted, the client is activated.

Specifies the client to be activated. `name` must refer to a previously configured client.

**Usage**

Activate clients after they have been configured or deactivated by the system or by configuration.

**Example**

```
activate client sampleClient
no activate client sampleClient
```
client

Configures/removes a client from the ORB element manager system interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
client id name [encrypted] password pwd
no client id name
```

Refer to the [syntax](#) documentation for more information.

no
Indicates the client specified is to be removed from the configuration.

```
id name
```

Specifies the client to be configured. *name* must be from 1 to 10 alpha and/or numeric characters in length.

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

```
password pwd
```

Specifies the password for the client. *pwd* must be from 1 to 35 alpha and/or numeric characters.

Usage

Clients for ORB element manager access must be configured prior to being activated.

Example

The following commands set the password for client *sampleClient* specifying a plain text password and an encrypted password as well.

```
client id sampleClient password secretPassword
client id sampleClient encryptedPassword f54gj801sd
```

The following deletes *sampleClient* from the configuration.

```
no client id sampleClient
```
default

Restores the system default values for the option specified.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
default \{ event-notif-iiop-port | event-notif-service filter | event-notif-siop-port | iiop-port | iop-address | max-attempt | session-timeout | siop-port \}
```

**event-notif-iiop-port**
Restores the port number for the inter-ORB event notifications to the system default: 7778.

**event-notif-service filter**
Restores the ORB Notification Service filter to its default behavior of sending all “error” level and higher events, and “info” level events for the orbs facility, CLI command logs, and license change logs.

**event-notif-siop-port**
Restores the port to use for secure socket layer inter-ORB event communication to the system default: 7777.

**iiop-port**
Restores the port number for the inter-ORB communications to the system default: 14132.

**iop-address**
Restores the IP address for the inter-ORB communications to the system default: IP address of current context.

**max-attempt**
Restores the maximum number of failed login attempts before which the client is deactivated to the system default: 3 attempts.

**session-timeout**
Restores the amount of idle time (no activity) before a session is terminated to the system default: 300 seconds.

**siop-port**
Restores the secure socket layer I/O port for inter-ORB events to the system default: 14131.

**Usage**

Restore the ORB element manager options to a well known values, the system defaults.
Example

default event-notif-i1op-port

default max-attempt
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
**event-notif-iiop-port**

Configures the port number for the Internet inter-ORB event notifications.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
event-notif-iiop-port number
```

*number*
Default: 7778
Specifies the port number to use as a number between 1 and 65535.

**Usage**
Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications. Event notification port configured is only used if the Internet inter-ORB transport is enabled via the `iiop-transport` command with the event notification service being enabled as well.

**Example**

```plaintext
event-notif-iiop-port 25466
```
event-notif-service

Enables/disables the ORB Notification Service and allows the configuration of filters dictating which event notifications are sent.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
(event-notif-service [filter {event-id event_id[to final_event_id] | facility event_facility_level event_level}] |
no event-notif-service [filter {event-id event_id[to final_event_id] | facility event_facility_level event_level}] )
```

no
Indicates the event notification service is to be disabled.

**event-id event_id [to final_event_id]**

Specifies an event filter based on event identification (event ID) number.
`event_id` is a specific event ID to filter or is the initial event ID in range if the `to` keyword is used. It can be configured to any integer value between 1 to 100,000.
`to` allows the specification of a range of event IDs to filter. When used, `final_event_id` specifies the last event ID in the range to be filtered. It can be configured to any integer value between 1 to 100,000 but should be a value greater than the initial event ID.

**facility event_facility_level event_level**

Specifies an event filter based on facility type and notification severity level.
`event_facility` specifies the facility type and can be any one of the following:
- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaprox**: AAA Proxy facility
- **acl-log**: Access Control List logging facility
- **acctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **all**: All facilities
ORBEM Configuration Mode Commands

- **asf**: Voice Application Server Framework logging facility
- **asfprt**: ASF Protocol Task (SIP) logging facility
- **asngwmgr**: ASN Gateway Manager facility
- **asnlrmgr**: ASN Paging/Location-Registry Manager facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **cli**: CLI logging facility
- **cscf**: IMS/MMD CSCF
- **cscfmgr**: SIP CSCF Manager facility
- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **dcardctr**: IPSEC Daughtercard Controller logging facility (not used at this time)
- **dcardmgr**: IPSEC Daughtercard Manager logging facility (Not used at this time)
- **dhcp**: DHCP facility (GGSN product only)
- **dhost**: Distributed Host logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-ecs**: ECS Diameter signaling facility
- **dpath**: IPSEC Data Path facility
- **drvctrl**: Driver Controller facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpe**: GTP-C protocol logging facility (GGSN product only)
- **gtpcmgr**: GTP-C protocol Manager logging facility (GGSN product only)
- **gtpp**: GTP-PRIME protocol logging facility (GGSN product only)
- **gtpu**: GTP-U protocol logging facility (GGSN product only)
- **h248prt**: H.248 Protocol logging facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **ims-authorizatn**: IMS Authorization Service facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipsec**: IP Security logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ips**: IP Pool Sharing Protocol logging facility
- **l2tp-control**: L2TP control logging facility
• l2tp-data: L2TP data logging facility
• l2tpdemux: L2TP Demux Manager logging facility
• l2tpmgr: L2TP Manager logging facility
• li: Lawful intercept facility (Logs are visible only to system accounts with li-administrator privileges.)
• mobile-ip: Mobile IP processes
• mobile-ip-data: Mobile IP data facility
• multicast-proxy: Multicast Proxy logging facility
• netwstrg: Network Storage facility
• npuctrl: Network Processor Unit Control facility
• npumgr: Network Processor Unit Manager facility
• nsctrl: Charging Service Controller facility (supported in conjunction with ECSv1)
• nsmgr: Charging Service Manager facility
• nsproc: Charging Service process facility
• orbs: Object Request Broker System logging facility
• ospf: OSPF logging facility
• ppp: PPP link and packet facilities
• radius-acct: RADIUS accounting logging facility
• radius-auth: RADIUS authentication logging facility
• radius-coa: RADIUS change of authorization and radius disconnect
• rct: Recovery Control Task logging facility
• rdt: Redirect Task logging facility
• resmgr: Resource Manager logging facility
• rip: RIP logging facility (RIP is not supported at this time.)
• rohc: RObust Header Compression facility
• rsvp: Reservation Protocol logging facility
• sct: Shared Configuration Task logging facility
• sessctrl: Session Controller logging facility
• sessmgr: Session Manager logging facility
• sft: Switch Fabric Task logging facility
• sipcdprt: Sip Call Distributor facility
• sitmain: System Initialization Task main logging facility
• snmp: SNMP logging facility
• srdb: Static Rating Database
• srp: Service Redundancy Protocol (SRP) logging facility
• ssh-ipse: SSH IP Security logging facility stat: Statistics logging facility
• stat: Statistics logging facility
• system: System logging facility
ORBEM Configuration Mode Commands

- tacacsplus: TACACS+ Protocol logging facility
- threshold: threshold logging facility
- udr: User detail record facility (used with the Charging Service)
- user-data: User data logging facility
- user-l3tunnel: User layer-3 tunnel logging facility
- vpn: Virtual Private Network logging facility
- wimax-data: WiMAX DATA
- wimax-r6: WiMAX R6

**event_notif-service**

---

*event_level* specifies the severity level of the event notification to filter and can be configured to one of the following:

- critical: display critical events
- error: display error events and all events with a higher severity level
- warning: display warning events and all events with a higher severity level
- unusual: display unusual events and all events with a higher severity level
- info: display info events and all events with a higher severity level
- trace: display trace events and all events with a higher severity level
- debug: display all events

**Usage**

This command is used to enable or disable the ORB Notification Service. Additionally, it can be used to configure filters dictating which events are sent. This service is disabled by default. Filters can be configured for a specific event identification number (event ID), a range of event IDs, or specific severity levels for events for particular facilities. When no filters are configured and the service is enabled, the ORB Notification Service sends all “error” level and higher events, and “info” level events for the orbs facility, CLI command logs, and license change logs.

Multiple instance of this command can be executed to configure multiple filters.

**Example**

The following command enables the ORB Notification service:

```
event-notif-service
```

The following command disables the ORB Notification service:

```
no event-notif-service
```

The following command configures a filter for the ORB Notification Service allowing only event IDs 800 through 805 to be sent:

```
event-notif-service filter event-id 800 to 805
```

The following command configures a filter for the ORB Notification Service allowing only “critical” level notifications for the A11 facility:

```
event-notif-service filter facility all level critical
```
**event-notif-siop-port**

Configures the port to use for secure socket layer inter-ORB event communication.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
event-notif-siop-port number
```

*number*
Default: 7777
Specifies the port number to use as a number between 1 and 65535.

**Usage**
Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications using SSL.

**Example**

```plaintext
event-notif-siop-port 25466
```
exit

Exits the ORBEM configuration mode and returns to the global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the global configuration mode.
**iiop-port**

Configures the port number for the internet inter-ORB communications.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] iiop-port number
```

- **no**
  
  Disables the iiop port.

- **number**
  
  Default: 14132
  
  Specifies the port number to use as a number between 1 and 65535.

**Usage**

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.

Internet inter-ORB port is only used if the Internet inter-ORB transport is enabled via the `iiop-transport` command.

**Example**

```
iiop-port 25466
```
iiop-transport

Enables/disables use of the Internet Inter-ORB Protocol for management across the network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
iiop-transport
no iiop-transport
```

no
Indicates no internet inter-ORB protocol communication is to take place across the network.

Usage
Enable the transport of Internet Inter-ORB Protocol messages to support remote management across the network.
The chassis is shipped from the factory with the Internet Inter-ORB transport disabled.

Example
The following commands enable and disable the ORB-based management across the network, respectively.

```
nioiop-transport
no iiop-transport
```
iop-address

Enables/disables use of the Internet Inter-ORB Protocol for management across the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
iop-address ip_address
```

*ip_address*
Specifies the IP address to use for inter-ORB communications for the current context. *ip_address* must be specified using the standard IPv4 dotted decimal notation.

**Usage**
Change the inter-ORB IP address when the IP address of the current context should not be used. The IP address of the local context may not be appropriate when the ORB configuration across nodes would cause conflicts with the IP addresses.

The chassis is shipped from the factory with the inter-ORB IP address defaulted to the IP address of the current context.

**Example**

```
iop-address 1.2.3.4
```
max-attempt

Configures the maximum number of failed login attempts before which the client is deactivated.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
max-attempt count
```

`count`

Default: 3 attempts

Specifies the number of failed login attempts prior to deactivating a client. The value must be within the range of 1 through 10.

**Usage**

Adjust the maximum number of attempts to a smaller value to increase the security level of the system.

**Example**

```
max-attempt 3
```
**session-timeout**

Configures the amount of idle time (no activity) before a client session is terminated.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
session-timeout seconds
```

*seconds*
Default: 300 seconds
Specifies the number of seconds of idle time before a client session is terminated. The value must be in the range of 1 through 86400.

**Usage**
Reduce the session timeout when the maximum number of sessions allowed is frequently being reached. Setting this to a lower value will help release idle sessions faster to allow use by other clients.

**Example**

```
session-timeout 1800
```
**siop-port**

Configures the secure socket layer I/O port for inter-ORB events.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
siop-port number
```

*number*

Default: 14131
Specifies the port number to use as a number between 1 and 65535.

**Usage**
Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications.

**Example**

```
siop-port 25466
```
ssl-auth-policy

Configures the secure socket layer peer authentication policy used by the ORBEM server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ssl-auth-policy { auth-none | auth-once | auth-once-fail | auth-peer | auth-peer-fail }

auth-none | auth-once | auth-once-fail | auth-peer | auth-peer-fail

Default: auth-none
auth-none: ORBEM server does not authenticate the peer
auth-once: ORBEM server authenticates the peer once (no fail)
auth-once-fail: ORBEM server authenticates the peer once (fail if no certificate)
auth-peer: ORBEM server authenticates the peer every time (no fail)
auth-peer-fail: ORBEM server authenticates the peer every time (fail if no certificate)

Usage
Use to configure the peer authentication policy used by the SSL transport of ORBEM.

Example
The following command sets the policy to authenticate the peer once without failure.
ssl-auth-policy auth-once
ssl-certificate

 Defines the certificate to be used by the SSL transport of ORBEM.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ssl-certificate { string certificate | file url }
```

**string certificate**

Specifies an ORBEM SSL certificate. `certificate` is a string of up to 4096 alpha and/or numeric characters.

**file url**

Default: /usr/ssl/certs/orbscert.pem

Specifies an ORBEM SSL certificate file and location. `url` is a string of up to 1024 alpha and/or numeric characters.

**Usage**

Use to configure the certificate to be used by the SSL transport of ORBEM. Note that if file option is used, the certificate content is read from the url and converted into quoted string.

**Example**

The following command defines the certificate cert3.pem file as being located in the `/usr/ssl/certs` directory:

```plaintext
ssl-certificate file /usr/ssl/certs/cert3.pem
```

The following command defines the certificate string (the string shown is abbreviated):

```plaintext
ssl-certificate string "-----BEGIN CERTIFICATE-----
MIIEJCCA5AwIBAgIBATANBgkqhkiG9w0BAQQFADCBsTELMAkGA1UEBhMCSVVMx
FjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxEjAQBgNVAcTCVRld2t2YnVyeTeeMBwG
A1UEChMVU3RhcmVudCBoZCXR3b3JrrcyBbmMuMlswIAYDVQQLExiFbGVtZW50I1h
bmFnZW1ib3JiZW1AbnVsaW5raW5jLmNvbzA6MB0GA1UEChMVU3RhcmVudCBOZCXR3b
3JrrcyBbmMuMlswIAYDVQQLExiFbGVtZW50I1h
b3JiZW1ib3JiZW1AbnVsaW5raW5jLmNvbzA6MBoGA1UEChMVU3RhcmVudCBOZCXR3b
3JrrcyBbmMuMlswIAYDVQQLExiFbGVtZW50I1h
b3JiZW1ib3JiZW1AbnVsaW5raW5jLmNvbzA6MGUGA1UEChMVU3RhcmVudCBOZCXR3b
3JrrcyBbmMuMlswIAYDVQQLExiFbGVtZW50I1h
b3JiZW1ib3JiZW1AbnVsaW5raW5jLmNvbzA6MIGUGA1UEChMVU3RhcmVudCBOZCXR3b
3JrrcyBbmMuMlswIAYDVQQLExiFbGVtZW50I1h
b3JiZW1ib3JiZW1AbnVsaW5raW5jLmNvbzA6MIIGDzAwBgNVBAMTB0Fsb29naW5hdXJh
b3JiZW1AbnVsaW5raW5jLmNvbzA6MIIGDwAwBgNVBAMTB0Fsb29naW5hdXJh
b3JiZW1AbnVsaW5raW5jLmNvbzA6MIIGDzAgBgNVBAMTB0Fsb29naW5hdXJh
b3JiZW1AbnVsaW5raW5jLmNvbzA6MIIGDwUwBgNVBAMTB0Fsb29naW5hdXJh
..."
```
ssl-certificate

```
Z5Fi8akXHhKhN7UMKyiW/Nn5NyfqPIA+9JwYMqwVOG8ybtfBQlGRCQodbXUm6Z9Z`

cM3XxWKVKHvoi83fJfpSLnuGkB1W8m3p/snHBH2BtgNT8OLtTdHedTKL72`

Z1xGF9/ok9hUqU4ikzQeEQ==`

-----END CERTIFICATE-----
```

Cisco ASR 5000 Series Command Line Interface Reference

3940

OL-22948-01
ssl-private-key

Configures the SSL private key used by the ORBEM server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

ssl-private-key { string key | file url }

string key
Specifies an ORBEM SSL private key. key is a string of up to 4096 alpha and/or numeric characters.

file url
Default: /usr/ssl/certs/orbscert.pem
Specifies the ORBEM SSL private key file location. url is a string of up to 1024 alpha and/or numeric characters.

Usage
Use to configure the private key to be used by the SSL transport of ORBEM. Note that if file option is used, the private key is read from the url and converted into quoted string.

Example
The following command defines the private-key cert3.pem file as being located in the /usr/ssl/certs directory:
ssl-private-key file /usr/ssl/certs/cert3.pem
The following command defines the private-key string (the string shown is abbreviated):
ssl-private-key string "-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC6Dh79iaK/zZG/Kwme2XS6G8/n3/+sac6huxI1WYammyYZKZp
n7qh720wpN4isqN7YfGLQoGslQhjS8z6ZT0ZUhyusYorE6yHTV23nHNtQIDAQAB
9br1iVWvy/N23WXzliH+e1tBiHqlSd/0wJBAEEOQH/vJse/YdHeYjIT76lGRe
Tq6ldBXdoLRDGUF2AqdboJ7wWCOJQO34XbBtmWfTkqz48Mi6uh3/5kDfH8CGQAl
XObwFPRztkvXprZrh7lckAxuoHiT1JsEKSIGPzEqDY2moWDgh0vPETO+5zEwQk
TXzLaRHgbly9MKnXSt8CQQCbrf77VndEFG9VWyPzeL4vx4ZhUMZQ6F1jOx7Xq9x
mZ8h4fcdg3ahlNt35gL/DjU7yd1+4MgLrRf3Udbk9
-----END RSA PRIVATE KEY-----"
Chapter 159
OSPF Configuration Mode Commands

The OSPF Configuration sub-mode is used to configure the OSPF routing protocol. This mode includes commands that configure OSPF routing parameters.

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

Enables authentication for the specified OSPF area.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
area {ipaddress|decimal_value} authentication [message-digest] no area {ipaddress|decimal_value} authentication [message-digest]
```

no

Disables authentication for the specified area.

ipaddress

The IP address, in IPv4 dotted-decimal notation, of the area where authentication will be enabled.

decimal-value

The identification number of the area where authentication will be enabled. This must be an integer from 0 through 4294967295.

message-digest

Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

Usage

Use this command to enable authentication of OSPF areas.

Example

The following command enables authentication for an OSPF area defined by the IP address 192.168.100.10 and the OSPF authentication type to MD5:

```
area 192.168.100.10 authentication message-digest
```
area default-cost

This command configures the default cost for an area.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
area { ipaddress | decimal_value } default-cost cost_value
no area { ipaddress | decimal_value } default-cost cost_value
```

**Usage**
Use this command to configure the default cost for an OSPF area.

**Example**
The following command sets the default cost for an OSPF area defined by the IP address 192.168.100.10 to 300:

```
area 192.168.100.10 default-cost 300
```
**area nssa**

Define an area as an NSSA (Not So Stubby Area) and configure OSPF parameters for it.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
area {ipaddress|decimal_value} nssa [default-information originate] [no redistribution no-summary] [translate always] [translate candidate] [translate never]
```

- **ipaddress**
The IP address, in IPv4 dotted-decimal notation, of the NSSA area.

- **decimal-value**
The identification number of the NSSA area. This must be an integer from 0 through 4294967295.

- **default-information originate**
Originating default information to the NSSA area.

- **no redistribution**
Do not redistribute external routes to the NSSA area.

- **no summary**
Do not inject inter-area routes into NSSA.

- **translate always**
Configure NSSA-ABR to always translate.

- **translate candidate**
Configure NSSA-ABR for translate election. (This is enabled by default.)

- **translate never**
Configure NSSA-ABR to never translate.

**Usage**

Use this command to define NSSA areas.

**Example**
The following command defines the area designated by the IP address 192.168.100.10 as an NSSA area:
area nssa

area 192.168.100.10 nssa
area stub

This command defines an area as a stub area.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
```
area { ipaddress | decimal_value } stub [ no-summary ]
```

**ipaddress**
The IP address, in IPv4 dotted-decimal notation, of the stub area.

**decimal_value**
The identification number of the stub area. This must be an integer from 0 through 4294967295.

**no-summary**
Disables (stops) the ABR from sending summary LSAs into the stub area.

Usage
Use this command to define an OSPF area as a stub area.

Example
The following command defines the OSPF area defined by the IP address 192.168.100.10 as a stub area:
```
area 192.168.100.10 stub
```
area virtual-link

This command configures a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product
- PDSN, HA, GGSN

Privilege
- Security Administrator, Administrator

Syntax

```
area { ipaddress|decimal_value} virtual-link router_id_address
```

- `ipaddress`
The IP address, in IPv4 dotted-decimal notation, of the transit area.

- `decimal-value`
The identification number of the transit area. This must be an integer from 0 through 4294967295.

- `router_id_address`
The router id, in dotted-decimal notation, of the ABR to be linked to.

Usage
Use this command to create a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example
The following command creates a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:
```
area 192.168.100.10 virtual-link 192.168.200.20
```
area virtual link authentication

This command configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

**Product**
- PDSN, HA, GGSN

**Privilege**
- Security Administrator, Administrator

**Syntax**

```plaintext
area {ipaddress|decimal_value} virtual-link router_id_address {message-digest | null | text }
```

- **ipaddress**
The IP address, in IPv4 dotted-decimal notation, of the transit area.

- **decimal-value**
The identification number of the transit area. This must be an integer from 0 through 4294967295.

- **router_id_address**
The router id, in dotted-decimal notation, of the ABR to be linked to.

- **message-digest**
Set the OSPF authentication type to use the message digest (MD) authentication method.

- **null**
Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

- **text**
Set the OSPF authentication type to use the clear text authentication method.

**Usage**
Use this command to set the authentication method for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

**Example**
The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to use no authentication:

```
area 192.168.100.10 virtual-link 192.168.200.2 null
```
area virtual-link authentication-key

This command configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
area {ipaddress|decimal_value} virtual-link router_id_address authentication-key [encrypted] password authentication_key

- **ipaddress**
The IP address, in IPv4 dotted-decimal notation, of the transit area.

- **decimal-value**
The identification number of the transit area. This must be an integer from 0 through 4294967295.

- **router_id_address**
The router id, in dotted-decimal notation, of the ABR to be linked to.

- **encrypted**
Use this if you are pasting a previously encrypted authentication key into the CLI command.

- **password authentication_key**
The password to use for authentication. **authentication_key** is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication password. This variable is entered in clear text format.

Usage
Use this command to specify the authentication password for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example
The following command creates an authentication password of 123456 for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:

area 192.168.100.10 virtual-link 192.168.200.20 authentication-key password 123456
area virtual link intervals

This command configures the interval or delay type, and the delay time in seconds, for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

area {ipaddress|decimal_value} virtual-link router_id_address[dead-interval value][hello-interval value][retransmit-interval value][transmit-delay value]

ipaddress
The IP address, in IPv4 dotted-decimal notation, of the area.

decimal-value
The identification number of the transit area. This must be an integer from 0 through 4294967295.

router_id_address
The router id, in dotted-decimal notation, of the ABR to be linked to.

dead-interval value
The interval, in seconds, that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. value must be an integer from 1 through 65535.

hello-interval value
The interval, in seconds before sending a hello packet. value must be an integer from 1 through 65535.

retransmit-interval value
The interval, in seconds, that router should wait before retransmitting a packet. value must be an integer from 1 through 65535.

transmit-delay value
The interval, in seconds, that the router should wait before transmitting a packet. value must be an integer from 1 through 65535.

Usage
Use this command to set the intervals or delay types for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.
Example
The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to 60 seconds:
area 192.168.100.10 virtual-link 192.168.200.20 retransmit-interval 60
area virtual link message-digest-key

This command enables the use of MD5-based OSPF authentication for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
```
area {ipaddress|decimal_value} virtual-link router_id_address message-digest-key key_id md5 [encrypted] password authentication_key
```

- **ipaddress**
The IP address, in IPv4 dotted-decimal notation, of the transit area.

- **decimal-value**
The identification number of the transit area. This must be an integer from 0 through 4294967295.

- **router_id_address**
The router id, in dotted-decimal notation, of the ABR to be linked to.

- **message-digest-key key_id**
Specifies the key identifier number. key_id must be an integer from 1 through 255.

- **encrypted**
Used this if you are pasting a previously encrypted authentication key into the CLI command.

- **password authentication_key**
The password to use for authentication. authentication_key is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication password. This variable is entered in clear text format.

Usage
Use this command to enable the use of MD5-based OSPF authentication for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example
The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20, sets the MD5 Key ID to 25, and the password to 123456:
```
area 192.168.100.10 virtual-link 192.168.200.20 message-digest-key 25 md5 password 123456
```
capability graceful-restart

This command configures graceful-restart. By default, capability is set to enabled.

**Product**
PDFN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
capability graceful-restart

   no capability graceful-restart

no

Disables capability graceful-restart.
```

**Usage**

Use this command to configure graceful-restart.

**Example**
The following command configure capability graceful-restart:

```plaintext
capability graceful-restart
```
default-information originate

This command creates a default external route into an OSPF routing domain.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
\[
\text{default-information originate [always][metric metric_value][metric-type \{1 | 2\}][route-map route_map_name]}
\]

always
Indicates that the route should always be advertised, regardless of whether the software has a default route or not.

metric metric_value
Sets the OSPF metric used in creating the default route. This must be an integer from 1 through 16777214.

metric-type \{1 | 2\}
Sets the default route metric type.
1 : Sets the OSPF external link type for default routes to Type 1.
2 : Sets the OSPF external link type for default routes to Type 2.

route-map route_map_name
Specifies the name of the default route-map to be used. This must be specified as a string of 1 through 79 alphanumeric characters.

Usage
Use this command to set the default external route into an OSPF routing domain.

Example
The following command sets the default external route to originate from the routemap named rmap1:
\[
\text{default-information originate route-map rmap1}
\]
default metric

This command configure the default metric value for the OSPF routing protocol.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
```
default-metric metric_value
```

- `metric_value`
  The metric value to set. This must be an integer from 1 through 16777214. The default metric value setting is 26385.

Usage
Use this command to set the default metric for routes.

Example
The following command sets the default metric to 235:
```
default-metric 235
```
distance

This command configures the OSPF route administrative distances for all OSPF route types or based on specific route type.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
distance*distance_value*|ospf [[external*distance_value*][inter-area*distance_value*][intra-area*distance_value*]]

distance_value
is an integer, ranging from 1 to 255, that sets OSPF route administrative distances. The default distance value is 110.

ospf { [ external*distance_value* ] [ inter-area*distance_value* ] [ intra-area*distance_value* ] }

Set the distance value for the specified route type.

external*distance_value* Set the OSPF route administrative distance for routes from other routing domains, learned by redistribution. This must be an integer from 1 through 255. The default is 110.

inter-area*distance_value* sets the OSPF route administrative distance for routes from one routing area to another. This must be an integer from 1 through 255. The default is 110.

intra-area*distance_value* sets the OSPF route administrative distance for all routes within an area. This must be an integer from 1 through 255. The default is 110.

Usage
Use this command to set the administrative distance for OSPF routes.

Example
The following command sets the administrative distance for all OSPF route types to $30$:
distance $30$


distribute-list

This command enables the filtering of networks in outgoing routing updates.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

distribute-list route_access_list out {connected|rip|static}

route_access_list
The name of the OSPF route access list to use. This is an alphanumeric string up to 63 characters in length.

connected
Filter connected routes.

rip
Filter RIP routes. (RIP is not supported at this time.)

static
Filter static routes.

Usage
Use this command to enable the filtering of outgoing route updates by using the specified route access list.

Example
The following command uses the route access list named ral1 to filter outgoing routing updates for all connected routes:
distribute-list ral1 out connected
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
   end

Usage
   Change the mode back to the Exec mode.
exit

Exits the NTP configuration mode and returns to the global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the global configuration mode.
**ip vrf**

This command configures the VRF instances for OSPF routing protocol.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip vrf vrf_name
no ip vrf vrf_name
```

**no**
Disables the VRF instances and removes the configured VRF context association for OSPF routing.

```
vrf_name
```

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

**Usage**

Use this command to configure the IP VRF forwarding also to associate the preconfigured VRF context with the specific tunnel interface.
This command creates and enters the OSPF VRF Configuration Mode if required to configure the VRF context instances for OSPF routing.

**Example**
The following command enables preconfigured VRF context instance `ospf_vrf1` for OSPF routing and enters the OSPF VRF Configuration mode:

`ip vrf ospf_vrf1`
neighbor

This command configures OSPF routers that interconnect to non-broadcast networks.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
neighbor ip_address[poll-interval poll_interval_value][priority priority_value]
```

**ip_address**
The interface IP address of the OSPF neighbor. This must be a valid IP address entered in dotted-decimal notation.

**poll-interval poll_interval_value**
Default: 120
Set the number of seconds in the dead neighbor polling interval. This must be an integer from 1 through 65535

**priority priority_value**
Default: 0
Set the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the IP address specified. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

Usage
Use this command to configure OSPF routers that connect to non-broadcast networks.

Example
The following command specifies an OSPF router neighbor with the IP address of 192.168.100.10:
```
neighbor 192.168.100.10
```
**network area**

This command enables OSPF on an interface and defines the OSPF area for that network.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
network network_ip_address/network_mask area {area_id|area_ip_address}
```

- network_ip_address/network_mask
  The network address and mask that specify the interface on which OSPF will be enabled. This is entered in dotted-decimal notation, followed by the “/” and the mask. Example: 192.168.1.0/24.

- area_id
  The OSPF area identification number for the specified network. This must be an integer from 0 through 4294967295.

- area_ip_address
  The IP address of the OSPF area for the specified network. This must be entered in dotted-decimal notation.

**Usage**

Use this command to specify the IP address of the network interface that the OSPF router will use.

**Example**

The following command specified that the OSPF router will use the interface at IP address 192.168.1.0 with a netmask of 24:

```
network 192.168.1.0/24
```
ospf graceful-restart

This command helps configure graceful-restart specific settings.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
ospf graceful-restart grace-period grace_period | helper never policy only-reload only-upgrade
```

- `grace-period grace_period`
  
  OSPF graceful restart grace period (seconds) is the time in which OSPF restarts, it should be and integer between 1 to 1800. Default grace period is 60 seconds.

- `helper never policy`
  
  Helps configure OSPF helper settings.
  
  `never`: Specifies never as helper.
  
  `policy { only-reload | only-upgrade }`: Allows ospf graceful-restart helper policy.
    
    - `only-reload`: Allows ospf graceful-restart helper policy only-reload.
    
    - `only-upgrade`: Allows ospf graceful-restart helper policy only-upgrade.

Usage

Use this command to configure graceful-restart specific settings.

Example

The following command sets the graceful restart grace period to 60 seconds:

```
ospf graceful-restart grace-period 60
ospf graceful-restart helper policy only-reload
ospf graceful-restart helper policy only-upgrade
```
ospf router-id

This command configures the router ID for the OSPF process.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
ospf router-id ip_address
```

*ip_address*
The router ID for the OSPF process. This must be an IP address entered in dotted-decimal notation

**Usage**
Use this command to set the router ID for the current OSPF router process.

**Example**
The following command sets the router ID to 192.168.200.1:
```
ospf router-id 192.168.200.1
```
passive-interface

This command enables the suppression of OSPF routing updates on the specific interface.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
passive-interface interface_name
```

interface_name
The name assigned to a logical interface within the specific context. An interface name can be from 1 through 79 alphanumeric characters.

Usage
Use this command to suppress router updates on an interface in the current context.

Example
The following command suppresses OSPF routing updates on the interface named Intfcl:

```
passive-interface Intfcl
```
redistribute

This command redistributes routes into OSPF. This means that any routes from another protocol are redistributed to OSPF neighbors using the OSPF protocol.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
redistribute { bgp | connected | rip | static } [metric metric_value] [metric-type {1 | 2}] [route-map route_map_name]

bgp
Specifies that BGP routes will be redistributed.

**Important:** BGP routing is only supported for use with the HA.

connected
Specifies that connected routes will be redistributed.

rip
Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

static
Specifies that static routes will be redistributed.

metric metric_value
Sets the OSPF metric used in the redistributed route. This must be an integer from 1 through 16777214.

metric-type {1 | 2}
Default: 2
Sets route metric type that is applied to redistributed routes.
1 : Sets the OSPF external link type for routes to Type 1.
2 : Sets the OSPF external link type for routes to Type 2.

route-map route_map_name
Filter routes through the specified route map before redistribution. route_map_name specifies the name of the route-map to use and must be specified as a string of 1 through 79 alphanumeric characters.

Usage
Use this command to define what routing protocols should have their routes redistributed into OSPF.
Example
The following command defines that BGP routes should be redistributed:
redistribute bgp
refresh timer

This command adjusts the OSPF refresh timer.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

`refresh timer value`

value

Default: 10
The minimum amount of time, in seconds, to wait before refreshing an LSA. This must be an integer from 10 through 1800.

Usage

Use this command to define the amount of time to wait before refreshing an LSA.

Example

The following command sets the refresh timer to 90 seconds:

```
refresh timer 90
```
router-id

This command configures the router ID for the OSPF process.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
router-id ip_address
```

- **ip_address**
  - The router ID for the OSPF process. This must be an IP address entered in dotted-decimal notation

**Usage**

Use this command to set the router ID for the current OSPF router process.

**Example**

The following command sets the router ID to **192.168.200.1**:

```
routing-id 192.168.200.1
```
timers spf

This command adjusts the SPF timers.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
  timers spf delay_value hold_time_value
```

- `delay_value`
  Default: 5
  The delay time, in seconds, between receiving changes to an SPF calculation. This must be an integer from 0 through 4294967295.

- `hold_time_value`
  Default: 10
  The hold time, in seconds, between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

**Usage**

Use this command to set the SPF delay and hold timers for the current OSPF router process.

**Example**

The following command sets the delay timer to 15 and the hold timer to 15:

```
timers spf 15 15
```
Chapter 160
OSPF VRF Configuration Mode Commands

The OSPF VRF Configuration sub-mode is used to configure the virtual routing and forwarding (VRF) context instances for OSPF routing protocol. This mode includes commands that configure VRF instance for OSPF routing parameters.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          router ospf
            OSPF Configuration Mode
              ip vrf vrf_name
                OSPF VRF Configuration Mode
```

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

This command configures the various parameters, including authentication, area identification, virtual link id, delay/interval values for the specified OSPF area using specific VRF instance.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

[no] area { ip_address | decimal_value } {authentication [ message-digest ] | default-cost cost_value | nssa [default-information-originate] [no-redistribution no-summary] [translate-always] [translate-candidate] [translate-never] | stub [no-summary] | virtual-link router_ip_address [authentication {message-digest | null | text}] [authentication-key {encrypted password encrypted_string | password password_string}] [message-digest-key key_id md5 [encrypted password encrypted_string | password password_string]})} [dead-interval] [hello-interval] [retransmit-interval] [transmit-delay]

no
Disables/removes configured parameters for the specified OSPF area using specific VRF instance.

ip_address
Specifies the IP address in IPv4 dotted-decimal notation, of the area where authentication will be enabled.

decimal_value
Specifies the identification number of the area where parameters to be configured. This must be an integer from 0 through 4294967295.

message-digest
Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

default-cost cost_value
Sets the default cost for an OSPF area.

cost_value is the default cost to be configured for the specified area and must be an integer from 0 through 16777215.

nssa [default-information-originate] [no-redistribution no-summary] [translate-always] [translate-candidate] [translate-never]
Configures and defines an area as an NSSA (Not So Stubby Area) and configures OSPF parameters for it.

default-information-originate: This optional keyword configures the OSPF VRF instances to originate default information to the NSSA area.

no-redistribution: This optional keyword configures the OSPF VRF instance to not to redistribute external routes to the NSSA area.
**no-summary**
This optional keyword configures the OSPF VRF instance to not to inject the inter-area routes into NSSA.

**translate-always**
This optional keyword configures the NSSA-ABR always to translate. By default this is disabled.

**translate-candidate**
This optional keyword configures the NSSA-ABR always to translate election. By default this is enabled.

**translate-never**
This optional keyword configures the NSSA-ABR never to translate. By default this is disabled.

---

**stub [no-summary]**
This keyword specifies an OSPF area as an stub area configures the NSSA-ABR never to translate. By default this is disabled.

no-summary: This optional keyword disables (stops) the ABR from sending summary LSAs into the stub area.

---

**virtual-link router_id**
Specifies the router identifier which provides a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone. 

*router_id* must be an IP address in IPv4 dotted-decimal notation of the ABR to be linked to.

---

**authentication {message-digest | null | text}**
Configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

message-digest: Set the OSPF authentication type to use the message digest (MD) authentication method.
null: Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.
text: Set the OSPF authentication type to use the clear text authentication method.

---

**authentication-key**
Configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

---

**message-digest-key key_id**
Specifies the MD key identifier number for virtual link connection.

*key_id* must be an integer from 1 through 255.

---

**md5**
Sets the message digest to MD5 for virtual link connection.

---

**[encrypted] password passwd_string**
Specifies the password required for virtual link connection authentications. The keyword **password** is optional and if specified **passwd_string** must be from 1 to 63 alpha and/or numeric characters. The password specified must be in an encrypted format if the optional keyword **encrypted** was specified. The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
**dead-interval value**
Specifies the dead interval, in seconds, that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. *value* must be an integer from 1 through 65535.

**hello-interval value**
Specifies the hello interval, in seconds before sending a hello packet. *value* must be an integer from 1 through 65535.

**retransmit-interval value**
Specifies the delay between retransmission, in seconds, that the router should wait before retransmitting a packet. *value* must be an integer from 1 through 65535.

**transmit-delay value**
Specifies the interval, in seconds, that the router should wait before transmitting a packet. *value* must be an integer from 1 through 65535.

**Usage**
Use this command to configure/set the various network/connection/authentication parameters of OSPF areas using specific VRF instance.

**Example**
The following command enables authentication for an OSPF area defined by the IP address 192.168.100.10 and the OSPF authentication type to MD5:

```
area 192.168.100.10 authentication message-digest
```

The following command sets the default cost for an OSPF area defined by the IP address 192.168.100.10 to 300:
The following command defines the area designated by the IP address 192.168.100.10 as an NSSA area where translation of NSSA candidate is enabled by default:
```
area 192.168.100.10 nssa
```

The following command defines the OSPF area defined by the IP address 192.168.100.10 as a stub area:
```
area 192.168.100.10 stub
```

The following command creates a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:
```
area 192.168.100.10 virtual-link 192.168.200.20
```

The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to use no authentication:
```
area 192.168.100.10 virtual-link 192.168.200.20 null
```

The following command creates an authentication password of 123456 for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:
```
area 192.168.100.10 virtual-link 192.168.200.20 authentication-key password 123456
```

The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20, sets the MD5 Key ID to 25, and the password to 123456:
```
area 192.168.100.10 virtual-link 192.168.200.20 authentication-key md5 password 123456
```

The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to 60 seconds:
area 192.168.100.10 virtual-link 192.168.200.20 retransmit-interval 60
default-information originate

This command creates a default external route into an OSPF routing domain.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default-information originate [always] [metric metric_value] [metric-type {1 | 2}] [route-map route_map_name]
```

- **always**
  Indicates that the route should always be advertised, regardless of whether the software has a default route or not.

- **metric metric_value**
  Sets the OSPF metric used in creating the default route. This must be an integer from 1 through 16777214.

- **metric-type {1 | 2}**
  Sets the default route metric type.
  1: Sets the OSPF external link type for default routes to Type 1.
  2: Sets the OSPF external link type for default routes to Type 2.

- **route-map route_map_name**
  Specifies the name of the default route-map to be use. This must be specified as a string of 1 through 79 alphanumeric characters.

**Usage**

Use this command to set the default external route into an OSPF routing domain.

**Example**

The following command sets the default external route to originate from the routemap named `rmap1`:

```
default-information originate route-map rmap1
```
default metric

This command configures the default metric value for the OSPF routing protocol.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
default-metric metric_value
```

- **metric_value**
  The metric value to set. This must be an integer from 1 through 16777214. The default metric value setting is 26385.

**Usage**
Use this command to set the default metric for routes.

**Example**
The following command sets the default metric to 235:

```plaintext
default-metric 235
```
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the NTP configuration mode and returns to the global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the global configuration mode.
neighbor

This command configures OSPF routers that interconnect to non-broadcast networks.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
neighbor ip_address [poll-interval poll_inter_value] [ priority priority_value]
```

- **ip_address**
The interface IP address of the OSPF neighbor. This must be an IP address entered in dotted-decimal notation.

- **poll-interval poll_inter_value**
  Default: 120
  Set the number of seconds in the dead neighbor polling interval. This must be an integer from 1 through 65535

- **priority priority_value**
  Default: 0
  Set the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the IP address specified. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

**Usage**
Use this command to configure OSPF routers that connect to non-broadcast networks.

**Example**
The following command specifies an OSPF router neighbor with the IP address of 192.168.100.10:

```
neighbor 192.168.100.10
```
network area

This command enables OSPF on an interface and defines the OSPF area for that network.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
network ip_address/ip_mask area {area_id | area_ip_address}
```

**ip_address/ip_mask**
The network address and mask that specify the interface on which OSPF will be enabled. This is entered in dotted-decimal notation, followed by the “/” and the mask. Example: 192.168.1.0/24.

**area_id**
The OSPF area identification number for the specified network. This must be an integer from 0 through 4294967295.

**area_ip_address**
The IP address of the OSPF area for the specified network. This must be entered in dotted-decimal notation.

Usage
Use this command to specify the IP address of the network interface that the OSPF router will use.

Example
The following command specified that the OSPF router will use the interface at IP address 192.168.1.0 with a netmask of 24:
```
network 192.168.1.0/24
```
**ospf router-id**

This command configures the router ID for the OSPF process.

**Product**

PDSN, HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ospf router-id ip_address
```

*ip_address*

The router ID for the OSPF process. This must be an IP address entered in dotted-decimal notation

**Usage**

Use this command to set the router ID for the current OSPF router process.

**Example**

The following command sets the router ID to 192.168.200.1:

```
ospf router-id 192.168.200.1
```
passive-interface

This command enables the suppression of OSPF routing updates on the specific interface.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
passive-interface interface_name
```

- **interface_name**
  The name assigned to a logical interface within the specific context. An interface name can be from 1 through 79 alphanumeric characters.

Usage
Use this command to suppress router updates on an interface in the current context.

Example
The following command suppresses OSPF routing updates on the interface named *IntfCl*:

```
passive-interface IntfCl
```
redistribute

This command redistributes routes into OSPF. This means that any routes from another protocol are redistributed to OSPF neighbors using the OSPF protocol.

**Product**
PDSN, HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
redistribute {bgp | connected | rip | static} [metric value] [metric-type {1 | 2}] [route-map route_map_name]
```

- **bgp**
  Specifies that BGP routes will be redistributed.

  **Important**: BGP routing is only supported for use with the HA.

- **connected**
  Specifies that connected routes will be redistributed.

- **rip**
  Specifies that RIP routes will be redistributed. (RIP is not supported at this stage.)

- **static**
  Specifies that static routes will be redistributed.

- **metric value**
  Sets the OSPF metric used in the redistributed route.
  Value must be an integer from 1 through 16777214.

- **metric-type {1 | 2}**
  Default: 2
  Sets route metric type that is applied to redistributed routes.
  1: Sets the OSPF external link type for routes to Type 1.
  2: Sets the OSPF external link type for routes to Type 2.

- **route-map route_map_name**
  Filter routes through the specified route map before redistribution. route_map_name specifies the name of the route-map to use and must be specified as a string of 1 through 79 alphanumeric characters.

**Usage**
Use this command to define what routing protocols should have their routes redistributed into OSPF.

Example
The following command defines that static routes should be redistributed in an OSPF area:

```
redistribute static
```
refresh timer

This command adjusts the OSPF refresh timer.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax
refresh timer value

value
Default: 10
The minimum amount of time, in seconds, to wait before refreshing an LSA. This must be an integer from 10 through 1800.

Usage
Use this command to define the amount of time to wait before refreshing an LSA.

Example
The following command sets the refresh timer to 90 seconds:
refresh timer 90
router-id

This command configures the router ID for the OSPF process.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
router-id ip_address
```

- `ip_address`:
  The router ID for the OSPF process. This must be an IP address entered in dotted-decimal notation.

Usage
Use this command to set the router ID for the current OSPF router process.

Example
The following command sets the router ID to `192.168.200.1`:

```
router-id 192.168.200.1
```
timers spf

This command adjusts the Shortest Path First (SPF) timers.

Product
PDSN, HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

timers spf delay_value hold_time_value

  delay_value
  Default: 5
  The delay time, in seconds, between receiving changes to an SPF calculation. This must be an integer from 0 through 4294967295.

  hold_time_value
  Default: 10
  The hold time, in seconds, between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

Usage
Use this command to set the SPF delay and hold timers for the current OSPF router process.

Example
The following command sets the delay timer to 15 and the hold timer to 15:

timers spf 15 15
Chapter 161
Out-Address Configuration Mode Commands

The Out-Address configuration mode provides the commands to configure the outgoing addresses for SCCP entities.

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

Exits the configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the Global configuration mode.
gt-address

Configures the SCCP short address.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gt-address gt_address

  gt_address
  A string of 1 to 15 digits to define the GT-address
```

Usage
Define the GT-address

Example

```
gt-address 010405525397
```
gt-format

The GT-format provides four formats that can be used during GTT.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
[gt-format] format_num
```

- `format_num`:
  1: Selects GT-format 1 options which include `nature-of-address` and `odd/even`. Once selected, the system enters GT-Format1 configuration mode.
  2: Selects GT-format2 options which include `translation-type`. Once selected, the system enters GT-Format2 configuration mode.
  3: Selects GT-format3 options which include `encoding-scheme`, `numbering-plan`, and `translation-type`. Once selected, the system enters GT-Format1 configuration mode.
  4: Selects GT-format4 options which include `encoding-scheme`, `nature-of-address`, `numbering-plan`, and `translation-type`. Once selected, the system enters GT-Format4 configuration mode.

Usage
Select the a GT-format that include encoding-scheme as part of the GTT process.

Example

```
gt-format 3
```
ni-indicator

Configures the National and International indicator to use during the GTT process.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
i-indicator ni_ind
```

- **ni_ind**
  Select one of the following as the appropriate type of national indicator for the address structure:
  - `national`
  - `international`

**Usage**
Select the international indicator to be used for out-going addresses.

**Example**

```
i-indicator international
```
point-code

Selects and configures the SS7-type point code for use with the out-going address.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
point-code pt_code
```

pt_code
Enter 1 to 11 digits in the point code format predefined during variant selection of GTT association.

Usage

Define an ITU point code to be used for out-going address processing.

Example

```
point-code 6.255.6
```
routing-indicator

Selects the type of routing and the indicator to be included in the out-going message.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
routing-indicator routing_ind
```

```
routing_ind
Select one of the following options:
  • gt: Inserts an indicator that identifies routing based on global title.
  • ssn: Inserts an indicator that identifies routing based on the subsystem number.
```

Usage
Select global title as the appropriate routing indicator.

Example

```
routing-indicator gt
```
ssf

Selects the subservice field as factor in the out-going address processing. `ssf` sets the network indicator in the subservice field for SS7 Message Signal Units (MSUs). The indicator carried in the message’s routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the national - international.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

`ssf sub_svc_fld`

**sub_svc_fld**
Select one of the following options:

- **international**: The network indicator identifies the message as international with a point code structure that does not match the national point code structure,

- **national**: The network indicator identifies the messages as having a national point code structure.

- **reserved**: Provides an alternate network indicator for national messages.

- **spare**: Provides an alternate network indicator for international messages.

Usage
Select the international NI for inclusion in out-going address subservice fields.

Example

`ssf international`
SSN

Selects the subsystem number to be included in the out-going message.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
ssn  sub_sys_num
```

```
sub_sys_num
Enter an integer from 1 to 255.
```

Usage
Use subsystem number 44 in the out-going address.

Example

```
ssn 44
```
Chapter 162
PDG Service Configuration Mode Commands

The PDG Service Configuration Mode is used to specify the properties required for the UEs in the WLAN (Wireless Local Access Network) to interface with the PDG/TTG.
aaa attribute

Sets the attributes that the system uses in AAA messages.

Product
TTG

Privilege
Security Administrator, Administrator

Syntax

aaa attribute { 3gpp-negotiated-qos-profile string }

no aaa attribute

------------------------
3gpp-negotiated-qos-profile string
------------------------
Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling. string must be in the range of 1 to 31 characters.

no aaa attribute
Removes a previously configured AAA attribute.

Usage
Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling.

Example
The following command specifies the 3GPP negotiated QoS profile to use during IMS emergency call handling:

```text
aaa attribute 3gpp-negotiated-qos-profile 100
```
associate sgtp-service

Identifies the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG. TTG functionality supports GTP-C (GTP control plane) messaging and GTP-U (GTP user data plane) messaging between the TTG and the GGSN over the Gn’ interface.

**Important:** This command can be used before the associated service instance is created and configured but care should be used to match the service names.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] associate sgtp-service sgtp_service_name [ context sgtp_context_name ]
```

- **no**
  - Removes the service association definition from the configuration.

- **sgtp-service sgtp_service_name**
  - Specifies which SGTP service configuration, by naming the SGTP service instance, to associate with this PDG service.
  - `sgtp_service_name` must be a string of 1 through 63 alpha and/or numeric characters with no spaces.

- **context sgtp_context_name**
  - Defines the context in which the SGTP service was created. If no context is specified, the current context is used.
  - `sgtp_context_name` must be a string of 1 through 63 alpha and/or numeric characters with no spaces.

**Usage**

Use this command to associate the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG.

**Example**

The following command associates SGTP service `sgtp_service_1` with this PDG service:

```
associate sgtp-service sgtp_service_1 context sgtp_context_1
```
certificate-selection

Configures the PDG/TTG to select the trusted certificate (and the private key for calculating the AUTH payload) to be included in the first IKE_AUTH message from the PDG/TTG based on the APN (Access Point Name). The selected certificate is associated with the APN included in the IDr payload of the first IKE_AUTH message from the UE.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
certificate-selection apn-based

no certificate-selection
default certificate-selection
```

**certificate-selection apn-based**

Selects a trusted certificate for the first IKE_AUTH message based on the APN.

**no certificate-selection**

Disables APN-based certificate selection and resumes sending a certificate bound to a crypto template.

**default certificate-selection**

Sets the default certificate selection method to a certificate bound to a crypto template.

**Usage**

Configures the PDG/TTG to select the trusted certificate to be included in the first IKE_AUTH message based on the APN.

**Example**

Use the following example to enable APN-based certificate selection:

```
certificate-selection apn-based
```
bind

Binds the PDG service IPv4 address to a crypto template and specifies the maximum number of sessions the PDG service supports.

Product: PDG/TTG

Privilege: Security Administrator, Administrator

Syntax:

```
bind address ipv4_address { crypto-template string} mode { ttg | pdg } [ max-sessions number]
```

```
no bind
```

no bind

Removes a previously configured binding.

---

**address**

Specifies the IPv4 address of the PDG service with which the UE attempts to establish an IKEv2/IPSec tunnel. This address must be a valid IP address within the context. This is a mandatory parameter.

---

**crypto-template string**

Specifies the name of the crypto template to be bound to the PDG service. This is the name of the IPSec policy to be used as a template for PDG/TTG subscriber session IPSec policies. The crypto template includes most of the IPSec and IKEv2 parameters for keepalive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per PDG service. This is a mandatory parameter.

*string* is any value from 0 - 127 alpha and/or numeric characters.

---

**mode { ttg | pdg }**

Default: There is no default value.

Specifies whether the PDG service provides TTG or PDG functionality, as follows:

- In TTG mode, PDN connectivity is provided through the GGSN. PDG functionality is provided by the combined TTG and GGSN.
- In PDG mode, PDN connectivity and PDG functionality are provided directly through the PDG service.

This is a mandatory parameter.

---

**Important:** PDG mode is not supported in this software release.

---

Dependencies:

When you configure the PDG service to be in TTG mode, you must also configure the SGTP service using the `associate sgtp-service` command, as the TTG needs to connect with the GGSN to complete the PDG functionality.
The following behaviors occur when the PDG service operates in TTG mode:

- If the SGTP service associated with PDG service is not configured, the PDG service is not started.
- If the SGTP service associated with PDG service is not started, the PDG service is not started.
- If the SGTP service associated with PDG service is stopped, the PDG service is stopped.
- If the SGTP service associated with PDG service is re-started, the PDG service is re-started.
- If the SGTP service is not yet configured, whenever the SGTP service is started, the PDG service is started.

Note that starting or stopping the PDG service has no impact on the SGTP service.

**max-sessions number**

Default: 1000000

Specifies the maximum number of sessions to be supported by the PDG service. 

`number` can be any integer value from 0 - 1000000. 

If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

**Usage**

Use this command in PDG Service Configuration Mode to bind the IP address used as the connection point for establishing IKEv2/IPSec sessions to a crypto template. You can also use it to define the maximum number of sessions the PDG service supports.

**Example**

The following command binds a PDG service with an IP address of 1.2.3.4 to the crypto template `crypto_template_1`, sets the mode to TTG, and sets the maximum number of sessions to 500000:

```
bind address 1.2.3.4 crypto-template crypto_template_1 mode ttg max-sessions 500000
```
ip gnp-qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Gn' interface in the uplink direction.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Syntax

ip gnp-qos-dscp { background dscp| conversational dscp| interactive dscp| streaming dscp| interactive [ traffic-handling-priority traffic_priority] { allocation-retention-priority allocation_retention_priority} } +

no ip gnp-qos-dscp { background dscp| conversational dscp| interactive dscp| streaming dscp| interactive [ traffic-handling-priority traffic_priority] { allocation-retention-priority allocation_retention_priority} } +

default ip gnp-qos-dscp

no

Disables the overriding of the ToS (Type of Service) field and enables the pass-through option.

background dscp

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP background class, in which the data transfer is not time-critical (for example, in e-mail exchanges). This traffic class is the lowest QoS.
dscp: Set the DSCP for the specified traffic class. See the dscp section below.

conversational dscp

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP conversational class, in which there is a constant flow of traffic in both the uplink and downlink direction. This traffic class is the highest QoS.
dscp: Set the DSCP for the specified traffic pattern. See the dscp section below.

interactive [ traffic-handling-priority traffic_priority ]

Specifies the DSCP marking to be used for packets of sessions subscribed to three possible traffic priorities in the 3GPP interactive class, in which there is an intermittent flow of packets in the uplink and downlink direction. This traffic class has a higher QoS than the background class, but not as high as the streaming class. traffic_priority is the 3GPP traffic handling priority and can be the integers 1,2 or 3.

allocation-retention-priority allocation_retention_priority

Specifies the DSCP for the interactive class if the allocation priority is present in the QoS profile.
allocation-retention-priority can be the integers 1, 2, or 3.
DSCP uses the values in the following table based on the traffic handling priority and allocation/retention priority if the allocation priority is present in the QoS profile.
Important: If you only configure DSCP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility however, it is recommended that you configure all three values.

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP streaming class, in which there is a constant flow of data in either in the uplink or downlink direction. This traffic class has a higher QoS than the interactive class, but not as high as the conversational class.

dscp: Set the DSCP for the specified traffic pattern. See the dscp section below.

default

- background: be
- interactive
- Traffic Priority 1: ef
- Traffic Priority 1: af21
- Traffic Priority 1: af21
- streaming: af11
- conversational: ef

Specifies the DSCP for the specified traffic pattern. dscp can be configured to any one of the following:

<table>
<thead>
<tr>
<th>DSCP Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>af11:</td>
<td>Assured Forwarding 11 per-hop-behavior (PHB)</td>
</tr>
<tr>
<td>af12:</td>
<td>Assured Forwarding 12 PHB</td>
</tr>
<tr>
<td>af13:</td>
<td>Assured Forwarding 13 PHB</td>
</tr>
<tr>
<td>af21:</td>
<td>Assured Forwarding 21 PHB</td>
</tr>
<tr>
<td>af22:</td>
<td>Assured Forwarding 22 PHB</td>
</tr>
<tr>
<td>af23:</td>
<td>Assured Forwarding 23 PHB</td>
</tr>
<tr>
<td>af31:</td>
<td>Assured Forwarding 31 PHB</td>
</tr>
<tr>
<td>af32:</td>
<td>Assured Forwarding 32 PHB</td>
</tr>
<tr>
<td>af33:</td>
<td>Assured Forwarding 33 PHB</td>
</tr>
<tr>
<td>af41:</td>
<td>Assured Forwarding 41 PHB</td>
</tr>
<tr>
<td>af42:</td>
<td>Assured Forwarding 42 PHB</td>
</tr>
<tr>
<td>af43:</td>
<td>Assured Forwarding 43 PHB</td>
</tr>
<tr>
<td>be:</td>
<td>Best effort forwarding PHB</td>
</tr>
<tr>
<td>ef:</td>
<td>Expedited forwarding PHB</td>
</tr>
</tbody>
</table>
More than one of the above keywords can be entered within a single command.

Usage

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they’re tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gnp’ interface(s).

The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>2</td>
<td>Class 1</td>
</tr>
<tr>
<td>3</td>
<td>Class 2</td>
</tr>
<tr>
<td>4</td>
<td>Class 3</td>
</tr>
<tr>
<td>5</td>
<td>Class 4</td>
</tr>
<tr>
<td>6</td>
<td>Express Forwarding (ef)</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP level for the streaming traffic pattern to be ef:

```
ip gnp-qos-dscp streaming ef
```

The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be ef, ef, af22, and af41, respectively:

```
ip gnp-qos-dscp conversational ef streaming ef interactive af22 background af41
```
ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Wu interface in the downlink direction.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Syntax

ip qos-dscp { background dscp | conversational dscp | interactive dscp | streaming dscp | interactive [ traffic-handling-priority traffic_priority ] { allocation-retention-priority allocation_retention_priority } } +

no ip qos-dscp { background dscp | conversational dscp | interactive dscp | streaming dscp | interactive [ traffic-handling-priority traffic_priority ] { allocation-retention-priority allocation_retention_priority } } +

default ip qos-dscp

no

Disables the overriding of the ToS (Type of Service) field and enables the pass-through option.

background dscp

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP background class, in which the data transfer is not time-critical (for example, in e-mail exchanges). This traffic class is the lowest QoS.

dscp: Set the DSCP for the specified traffic class. See the dscp section below.

conversational dscp

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP conversational class, in which there is a constant flow of traffic in both the uplink and downlink direction. This traffic class is the highest QoS.

dscp: Set the DSCP for the specified traffic pattern. See the dscp section below.

interactive [ traffic-handling-priority traffic_priority ]

Specifies the DSCP marking to be used for packets of sessions subscribed to three possible traffic priorities in the 3GPP interactive class, in which there is an intermittent flow of packets in the uplink and downlink direction. This traffic class has a higher QoS than the background class, but not as high as the streaming class.

traffic_priority is the 3GPP traffic handling priority and can be the integers 1, 2 or 3.

allocation-retention-priority allocation_retention_priority

Specifies the DSCP for the interactive class if the allocation priority is present in the QoS profile.

allocation-retention-priority can be the integers 1, 2, or 3.

DSCP uses the values in the following table based on the traffic handling priority and allocation/retention priority if the allocation priority is present in the QoS profile.
<table>
<thead>
<tr>
<th>Allocation Priority</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Handling Priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>2</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
</tbody>
</table>

**Important:** If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility however, it is recommended that you configure all three values.

**streaming dscp**

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP streaming class, in which there is a constant flow of data in either the uplink or downlink direction. This traffic class has a higher QoS than the interactive class, but not as high as the conversational class.

`dscp`: Set the DSCP for the specified traffic pattern. See the `dscp` section below.

**dscp**

Default:
- background: be
- interactive
- Traffic Priority 1: ef
- Traffic Priority 1: af21
- Traffic Priority 1: af21
- streaming: af1
- conversational: ef

Specifies the DSCP for the specified traffic pattern. `dscp` can be configured to any one of the following:

<table>
<thead>
<tr>
<th>dscp</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>af11: Assured Forwarding 11 per-hop-behavior (PHB)</td>
<td>af33: Assured Forwarding 33 PHB</td>
</tr>
<tr>
<td>af12: Assured Forwarding 12 PHB</td>
<td>af41: Assured Forwarding 41 PHB</td>
</tr>
<tr>
<td>af13: Assured Forwarding 13 PHB</td>
<td>af42: Assured Forwarding 42 PHB</td>
</tr>
<tr>
<td>af21: Assured Forwarding 21 PHB</td>
<td>af43: Assured Forwarding 43 PHB</td>
</tr>
<tr>
<td>af22: Assured Forwarding 22 PHB</td>
<td>be: Best effort forwarding PHB</td>
</tr>
<tr>
<td>af23: Assured Forwarding 23 PHB</td>
<td>ef: Expedited forwarding PHB</td>
</tr>
<tr>
<td>af31: Assured Forwarding 31 PHB</td>
<td></td>
</tr>
<tr>
<td>af32: Assured Forwarding 32 PHB</td>
<td></td>
</tr>
</tbody>
</table>
More than one of the above keywords can be entered within a single command.

**Usage**

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they’re tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Wu interface(s). The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>2</td>
<td>Class 1</td>
</tr>
<tr>
<td>3</td>
<td>Class 2</td>
</tr>
<tr>
<td>4</td>
<td>Class 3</td>
</tr>
<tr>
<td>5</td>
<td>Class 4</td>
</tr>
<tr>
<td>6</td>
<td>Express Forwarding (ef)</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

**Example**
The following command configures the DSCP level for the streaming traffic pattern to be ef:

```
ip qos-dscp streaming ef
```

The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be ef, ef, af22, and af41, respectively:

```
ip qos-dscp conversational ef streaming ef interactive af22 background af41
```
ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip source-violation { clear-on-valid-packet | drop-limit num period secs }
default ip source-violation { drop-limit num period secs }
no ip source-violation clear-on-valid-packet
```

---

**clear-on-valid-packet**
Default: disabled
Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet.

---

**drop-limit num**
Default: 10
Sets the maximum number of allowed IP source violations within the detection period before dropping a call. If num is not specified, the value is set to the default value.
num can be any integer value from 1 to 1000000.

---

**period secs**
Default: 120
Sets the detection period in seconds for IP source violations. If secs is not specified, the value is set to the default value.
secs can be any integer value from 1 to 1000000.

---

**default ip source-violation { drop-limit num period secs }**
Sets or restores the IP source violation detection defaults, as follows:
drop-limit: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.
period: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

---

**no ip source-violation clear-on-valid-packet**
The drop-limit counters are not reset upon receipt of a properly addressed packet.

---

**Usage**
Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.
Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session. This function operates in the following manner: When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment. For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

Example
The following command sets the drop limit to 15 and leaves the other values at their default values:

```
ip source-violation drop-limit 15
```
max-tunnels-per-ue

The maximum number of IKEv2/IPSec tunnels allowed per UE by the PDG/TTG. This maximum number is specified per PDG service.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
max-tunnels-per-ue integer
```

default max-tunnels-per-ue

```
integer
Default: 11
The maximum number of IKEv2/IPSec tunnels allowed per UE. This value must be an integer from 1 to 11.
```

```
default max-tunnels-per-ue
Sets the maximum number of IKEv2/IPSec tunnels allowed per UE to its default value, which is 11.
```

**Usage**
Use this command to set the maximum number of IKEv2/IPSec tunnels allowed per UE.

**Example**
Use the following command to set the maximum number of IKEv2/IPSec tunnels allowed per UE to 2:
```
max-tunnels-per-ue 2
```

plmn id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Syntax

```
plmn id mcc mcc_number mnc mnc_number
no plmn id mcc mcc_number mnc mnc_number
```

**mcc mnc_number**

Specifies the mobile country code (MCC) portion of the PLMN’s identifier.
mcc_number is the PLMN MCC identifier and can be configured to any integer value between 200 and 999.

**mnc mnc_number**

Specifies the mobile network code (MNC) portion of the PLMN’s identifier.
mnc_number is the PLMN MNC identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.

**no plmn id mcc mcc_number mnc mnc_number**

Removes a previously configured PLMN identifier for the PDG service.

Usage

The PLMN ID is included in the RAI (Routing Area Identity) field of the PDP Create Request messages sent to the GGSN. Multiple PDG services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each PDG service.

Example

The following command configures the PLMN identifier with an MCC of 462 and MNC of 02:

```
plmn id mcc 462 mnc 02
```
**setup-timeout**

Specifies the maximum time allowed to set up a session in seconds.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
setup-timeout integer

default setup-timeout
```

---

**setup-timeout integer**

Default: 60
Sets the session setup timeout value.
integer is a value in the range of 2 - 300 seconds.

**default setup-timeout**

Sets or restores the default session setup timer value to 60 seconds.

---

**Usage**
The PDG/TTG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

---

**Example**
The following command sets the session setup timeout value to the default value of 60 seconds:

```
default setup-timeout
```
The PDIF Service Configuration Mode is used to configure the properties required for a mobile station to interface with a PDIF.

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

Sets the system attributes for AAA messages.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

aaa attribute { 3gpp2-bsid string | 3gpp2-service-option integer | calling-station-id integer | 3gpp2-serving-pcf <ip-address> }

no aaa attribute

default aaa attribute 3gpp2-service-option integer

no
Removes a previously configured AAA attribute.

default
Returns the specified aaa attribute to the original default system settings.

3gpp2-bsid string
Specifies the base-station ID and consists of the SID + NID + CELLID.
string must contain 12 hexadecimal upper-case ASCII characters.

3gpp2-service-option integer
Default: 4095
Specifies the radius attribute value when sending authentication and accounting messages.
integer can be configured to any value in the range 0 - 32767

calling-station-id integer
Calling station phone number.
integer can be configured to any value from 1 - 15 numbers.

3gpp2-serving-pcf
Use this command to generate attribute values without creating a new ASR 5000 image.

Usage
If the RADIUS protocol is being used, accounting messages can be sent over a AAA interface to the RADIUS server.
3gpp2-serving-pcf attribute value (if configured) is sent in both RADIUS authentication and accounting messages. If the attribute value is not configured (or explicitly 'not configured' using no command), radius
attributes are still included with just type and length. This is because inclusion/exclusion of radius attributes are still controlled through the dictionary, not with CLI.

Example
The following command identifies the base station ID:

```plaintext
aaa attribute 3gpp2-bsid 0ab23289acb3
```
aaa authentication

Sets the aaa authentication for first and second phase authentication when multiple authentication is configured on the system.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

aaa authentication { { first-phase | second-phase } | { context-name name aaa-group name } }

no aaa authentication { first-phase | second-phase }

no aaa authentication { first-phase | second-phase }

Removes any existing authentication configuration.

first-phase context-name name aaa-group name

Specifies the context name and the aaa group name configured in the context for the first authentication phase.
context-name name: Context where aaa server group is defined. name must be a string of size 1-79.
aaa-group name: Name of the aaa-group to be used for authentication. name must be a string of size 1-63.

second-phase context-name name aaa-group name

Specifies the context name and the aaa group name configured in the context for the second authentication phase.
context-name name: Context where aaa server group is defined. name must be a string of size 1-79.
aaa-group name: Name of the aaa-group to be used for authentication. name must be a string of size 1-63.

Usage

Two phase-authentication happens in IKEv2 setup for setting up the IPSec session. The first authentication uses Diameter AAA EAP method and second authentication uses RADIUS AAA authentication. The same AAA context may be used for both authentications. PDIF service allows you to specify only a single AAA group, which could normally be used for the first authentication method.
A given AAA group only supports either Diameter or RADIUS authentication. If the NAI in the first authentication is different from NAI in the second authentication each NAI can point to a different domain profile in the PDIF. Each domain profile may be configured with each AAA group, one for Diameter and the other for RADIUS.

Example

Use the following to configure first-phase authentication for an aaa group named aaa-10 in the pdif context:
first-phase context-name pdif aaa-group aaa-10
bind

Binds the service IP address to crypto template and configures the number of sessions the PDIF can support.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

bind address address { crypto-template string } [ max-sessions number ]

no bind

no
Removes a previously configured binding.

address
Specifies the IP address of the service.

crypto-template string
Specifies the name of the crypto template to be bound to the service.
string is any value from 0 - 127 alpha and/or numeric characters.

max-sessions number
Default is 3000000
Specifies the maximum number of sessions to be supported by the service.
number can be any integer value from 0 - 300000

Usage
Binds the IP address used as the connection point for establishing the IKEv2 sessions to the crypto template. It can also define the number of sessions the PDIF can support.

Example
The following command binds a service with the ip address 13.1.1.1 to the crypto template T1 and sets the maximum number of sessions to 200000:

    bind address 13.1.1.1 crypto-template T1 max-sessions 200000
default

Sets or restores the default condition for the selected parameter.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Syntax**

```
default { ( aaa attribute 3gpp2-service-option ) | duplicate-session-detection |
            hss ( failure-handling mac-address-validation-failure | mac-address-validation |
                  update-profile ) | ip source-violation ( drop-limit | period ) | setup-timeout |
            subscriber name | username mac-address-stripping ) }
```

**aaa attribute 3gpp2-service-option**

Configures the default value to 4095.

**duplicate-session-detection**

Configures the default to be NAI-based.

**hss { failure-handling mac-address-validation-failure | mac-address-validation |
        update-profile }**

Configures the HSS server defaults:
- **failure-handling mac-address-validation-failure**: By default, the MAC address is validated by IMS-Sh interface.
- **mac-address-validation**: By default, validating the MAC address is disabled.
- **update-profile**: By default, updating the PDIF profile is disabled.

**ip source-violation ( drop-limit | period )**

Configures IP source-violation detection defaults.
- **drop-limit**: Default number of ip source violations permitted in detection period before the call is dropped is 10.
- **period**: Default detection period is 120 seconds.

**setup-timeout**

Default call setup time limit is 60 seconds.

**subscriber name**

Configures the default subscriber name. *name* is a string of 1-127 characters.

**username mac-address-stripping**

Default is to disable stripping the MAC address from the username.
Usage
Configures the default settings for a given parameter.

Example
Use the following example to configure the default call setup time limit:

```
default setup-timeout
```
**duplicate-session-detection**

Configures the PDIF to detect duplicate call sessions using old IMSI or NAI addresses and clear old call information.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | default ] duplicate-session-detection { imsi-based | nai-based }
```

- **no**
  Stops duplicate session detection.

- **default**
  Configures the default setting, which is NAI-based detection.

- **imsi-based**
  Configures the PDIF to detect duplicate call sessions based on the IMSI address.

- **nai-based**
  Configures the PDIF to detect duplicate call sessions based on the NAI address. This is the default setting.

**Usage**

If an MS leaves the Wi-Fi coverage area and subsequently comes back online, it may initiate a new session setup procedure. After both the device authentication with HSS and the subscriber authentication with AAA server are completed, PDIF runs the internal mechanism to see whether there was any other session bound with the same IMSI. If an old session is detected, PDIF starts clearing this old session by sending a proxy-MIP Deregistration request to the HA. PDIF resumes new session setup by sending a proxy-MIP registration request. When the old session is aborted, PDIF sends Diameter STR messages and RADIUS Acct STOP messages to corresponding AAA servers.

PDIF allows duplicate session detection based on either the NAI or IMSI addresses. When detecting based on NAI, it is the first-phase (device authentication) NAI that is used.

**Example**
The following command configures duplicate session detection to use IMSI addressing:

```
duplicate-session-detection imsi
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the previous mode.
hss

Configures the HSS server parameters.

Product: PDIF

Privilege: Security Administrator, Administrator

Syntax:

```
no
Removes a previously configured HSS profile.

default
Resets the defaults for this command.

failure-handling mac-address-validation-failure
Configures the way the HSS server is to handle errors.
If HSS returns a list of MAC addresses and if PDIF fails to match the subscriber MAC address against the
list, then the session is always terminated.

action { continue | terminate }
Configures the action to be performed depending on the failure type.
continue: Ignore a mac-address-validation-failure and continue the session.
terminate: Terminate the session on a mac-address-validation-failure.

mac-address-validation
Default: disabled
If mac-address-validation is enabled, the PDIF queries the HSS server for a list of MAC addresses associated
with the Mobile Directory Number (MDN).

update-profile
Default: disabled.
Update the HSS server with the subscriber profile.
```

Usage:

An HSS server is used to provide MAC address validation and store part of the subscriber profile. This
command enables or disables validation and profile updates, and configures how the system responds to
failures: terminate or continue a session.
An ims-sh-service and Diameter interface needs to be configured to communicate with the HSS server.

**Example**
The following example enables mac-address validation:

```
hss mac-address-validation
```
**ims-sh-service**

Associates the IMS-Sh-service parameters.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ims-sh-service name name

no ims-sh-service name name
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Removes a previously configured IMS-Sh-service.

<table>
<thead>
<tr>
<th>name</th>
</tr>
</thead>
</table>
| Names the IMS-Sh-service in the pdif-service context.

**Usage**

This command is used to name the IMS-Sh-service.

**Example**

The following command names the IMS-Sh-service ims1:

```plaintext
ims-sh-service name ims1
```
ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs }
no ip source-violation clear-on-valid-packet
```

**clear-on-valid-packet**

Default: disabled
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

**drop-limit num**

Default: 10
Sets the number of allowed source violations within a detection period before forcing a call disconnect. If *num* is not specified, the value is set to the default.

*num* can be any integer value from 1 to 1000000.

**period secs**

Default: 120
The length of time, in seconds, for a source violation detection period to last.

If *secs* is not specified, the value is set to the default.

*secs* can be any integer value from 1 to 1000000.

Usage

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDIFs a number of times during a handoff scenario.

This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments the IP source-violation drop-limit counter and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the drop-limit counter to increment.

For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The period timer continues to count throughout this process.

Example

The following command sets the drop limit to 15 and leaves the other values at their defaults:
ip source-violation drop-limit 15
**mobile-ip**

Sets the MIP FA context for the specific PDIF service.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
mobile-ip foreign-agent context string [ fa-service string ]
no mobile-ip
```

- **no**
  Removes previously configured parameters.

- **foreign-agent context string**
  Provides the context name in which the FA is configured. *string* is any value in the range 1 - 79 alpha and/or numeric characters.

- **fa-service string**
  Designates the name of the FA service in the FA context. *string* is any value in the range 1 - 79 alpha and/or numeric characters.

**Usage**

Shows in which context the FA is located and names the FA service.

**Example**

This command configures MIP for the FA context named fa1:

```
mobile-ip foreign-agent context fa1
```
setup-timeout

Configures the maximum time allowed to set up a session.

Product
PDIF

Privilege
Security-Administrator, Administrator

Syntax

setup-timeout integer

default setup-timeout

default
Default session setup timer: 60 seconds.

setup-timeout integer
This command manually sets the session setup timer. integer is a value in the range 2 - 300 seconds.

Usage
PDIF clears both user session and tunnels if a call does not initiate successfully before the timer expires.

Example
The following command sets the setup-timeout to the default 30 seconds:

default setup-timeout
username

Configures mac-address-stripping on a username coming in from a mobile station session.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
username mac-address-stripping
[ default | no ] username mac-address-stripping

no
Returns the configuration to the default condition.

default
Configures the parameter default, which is disabled.

mac-address-stripping
Configures mac-address stripping from the Network Access Identifier (NAI).
```

**Usage**

When enabled, PDIF strips the MAC address from a mobile username NAI before sending to the RADIUS AAA server.

**Example**
The following example disables mac-address-stripping.

```
no username mac-address-stripping
```
Chapter 164
PDSN Service Configuration Mode Commands

The PDSN Service Configuration Mode is used to create and manage PDSN service instances for the current context.
aaa 3gpp2-service-option

Specifies the value for the 3gpp2-service option.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

aaa 3gpp2-service-option number
no aaa 3gpp2-service-option number

Usage
Disables the aaa 3gpp2-service option configuration.

Usage
Allows the configuration of a default service option value to be sent in accounting when service option values are not received from PCF. The PDSN will default the service option value to the configured value if the value is not specified by the PCF.

Example
The following command sets the service option to be 40:

aaa 3gpp2-service-option 40
access-flow traffic-validation

if access-flow traffic-validation is enabled for the service and the subscriber then the flows are checked against the filter rules. If the packets does not match the filter rules, and N violations occur in K seconds, the rp connection is downgraded to best-effort flow, if it is not already a best-effort flow

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

access-flow traffic-validation threshold violations limit interval seconds

[no | default] access-flow traffic-validation

[no | default]
Disable traffic validation for the service.

threshold { [violations limit] [interval seconds]}
violations limit: Sets the parameters that determine traffic access violations. This is determined by setting the maximum number of violations within a set time period. must be an integer from 1 through 100000.
interval seconds: Sets the time interval, in seconds. must be an integer from 1 through 100000.

Usage
Use this command to enable traffic validation for the current PDSN service.

Example
The following command enables traffic validation for the current PDSN service and sets the limit allowed to 100 violations within 5 seconds:

access-flow traffic-validation threshold violations 100 interval 5
access-network

Configures access network parameters.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
access-network { accounting identifier | realm realm_name }
```

**accounting identifier**
Configures accounting for the access-network. This value must be a string from 1 to 128 characters in length.

**realm realm_name**
Configures the realm for the access-network. `realm_name` must be a string from 1 to 128 characters in length.

**Usage**
Use this command to configure access-network parameters for accounting and realms.

**Example**
The following command creates an `access-network realm` named `realm2`.

```plaintext
access-network realm realm2
```
airlink bad-sequence-number

Configures PDSN behavior for airlink related parameters.

Product
PDSN

Privilege
Security Administrator, Administrator

```
airlink bad-sequence-number {accept | deny [use-deny-code {poorly-formed-request | unsupported-vendor-id}]}[no | default] airlink bad-sequence-number
```

[no | default]
Disables the deny of bad-sequence number and accept it.
It is the default behavior.

**accept**
Accepts the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.
It is the default behavior.

**deny**
Rejects the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.
It uses **poorly-formed-request** option by default to deny a request.

**use-deny-code {poorly-formed-request | unsupported-vendor-id}**
These are optional keywords that used with **deny** sub-command to deny the A11 RRQ messages that have either an unsupported vendor Id or A11 Requests with bad/poor formation.
**unsupported-vendor-id** denies request on the basis of vendor Id.
**poorly-formed-request** will deny the A11 request on the basis of request formation or structure. It is the default deny code for **deny** sub-command.

**Usage**
This command is used to configure the airlink parameters for A11 RRQs.
When configured it denies the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

**Example**
The following command would configure the system to deny all A11 RRQ messages having unsupported vendor Id or bad structure of message, including those having airlink sequence number less than or equal to a previously received sequence number:

```
airlink bad-sequence-number deny
```
allow alt-ppp

Allows proprietary modified versions of PPP type sessions to connect this PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
allow alt-ppp
no allow alt-ppp
```

Usage

This command is used to deviate from standard PPP protocol and use a proprietary modified version of PPP with a pre-defined non-negotiable PPP parameters. It is a vendor-specific licensed feature command.
always-on-indication

Enables/disables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax
always-on-indication

no always-on-indication

Usage
This command is available when the 3GPP2 Always-On RP Extensions feature-use license is installed. When enabled, this command causes the PDSN service to include the Always On Indicators in the Normal Vendor Specific Extension (NVSE) part of an A11 Session Update message to the PCF. The indicator will only be sent for those subscriber sessions in which Always On functionality is enabled as determined after a successful authentication: the 3GPP2-Always-On attribute is set to a value of 1 (Active) for subscribers configured on a AAA server, or the always-on parameter is set for locally configured subscribers. This functionality is enabled by default.
authentication

Configures the PDSN service authentication parameters.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
authentication { { [ allow-noauth ] [ chap chap_priority ] [ mschap
mschap_priority ] [ pap pap_priority ] } | msid-auth }
```

---

**allow-noauth**

Default: Disabled
This option configures the system to provide subscribers with network access even though they have not been authenticated. This command issued by itself would cause the system to not attempt to authenticate subscribers.

When the allow-noauth option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system will treat the allow-noauth option as the lowest priority.

If no authentication is allowed, then NAI construct will be implemented in order to provide accounting records for the subscriber.

---

**chap chap_priority**

Default: 1
This option configures the system to attempt to use the Challenge Handshake Authentication Protocol (CHAP) to authenticate the subscriber.

A `chap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

`chap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference.

CHAP is enabled by default as the highest preference.

---

**mschap mschap_priority**

Default: Disabled
This option configures the system to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber.

A `mschap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

`mschap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference.

---

**pap pap_priority**

Default: 2
This option configures the system to attempt to use the Password Authentication Protocol (PAP) to authenticate the subscriber.
A `pap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. `pap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

### msid-auth

Default: Disabled

This option configures the system to attempt to authenticate the subscriber based on their Mobile Station Identity (MSID).

#### Usage

Use to specify how the PDSN service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.

The chassis is shipped from the factory with the authentication options set as follows:
- `allow-noauth` disabled
- `chap` enabled with a priority of 1
- `mschap` disabled
- `msid-auth` disabled
- `pap` enabled with a priority of 2

**Important:** At least one of the keywords must be used to complete the command.

#### Example

The following command would configure the system to allow no authentication for subscribers and would perform accounting using the default NAI-construct of `username@domain`:

```
authentication allow-noauth
```

The following command would configure the system to attempt subscriber authentication first using CHAP, then MSCHAP, and finally PAP. If the `allow-noauth` command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```
bind

Binds the PDSN service to a logical IP interface serving as the R-P interface. Specifies the maximum number of subscribers that can access this service over the interface.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

bind address address [ max-subscribers count ]

no bind address address max-subscribers max#

- **no**
  Removes a previously configured binding.

- **address**
  Specifies the IP address (address) of the interface configured as the R-P interface. address is specified in dotted decimal notation.

- **max-subscribers count**
  Default: 500000
  Specifies the maximum number of subscribers that can access this service on this interface.

- **count** can be configured to any integer value between 0 and 500,000.

**Important:** The maximum number of subscribers supported is dependant on the license key and the number of active PACs/PSCs installed in the system. A fully loaded system with 13 active PACs/PSCs can support 500,000 total subscribers. Refer to the license key command for additional information.

**Usage**

Associate or tie the PDSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an R-P interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of interfaces that you will configure for use as R-P interfaces
- The maximum number of subscriber sessions that all of the interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port (10/100Base-Tx or 1000Base-T) to which these interfaces will be bound
Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example
The following command would bind the logical IP interface with the address of 192.168.3.1 to the PDSN service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```plaintext
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```plaintext
no bind address
```
 bcmcs

Sets the BCMCS group username and password for RADIUS access.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
bcmcs { custom | flow-id value { header-compression rohc { rohc-profile name name } } | grpusrname group_name | [ encrypted ] grppassword group_password | ptt {destination-context disconnect-dscp-label rohc-profile-name}}
```

custom
Customise the BCMCS configuration.

flow-id value
Set the BCMCS flow-id. This value must be a hex string between 0x1000 and 0xFFFFFFFF. Making this entry opens a new mode: bcmcs-flow-id.

header-compression rohc Configure ROHC parameters.
rohc-profile name name: Configure ROHC parameters name, name should be string of size 1 to 63.

grpusrname group_name
Sets the BCMCS group name for RADIUS access requests. This value must be a string from 1 to 127 characters in length.

[ encrypted ] grppassword group_password
Set the BCMCS group password for RADIUS access requests. This value must be a string from 1 to 63 characters in length.
Password can be encrypted or clear.

ptt {destination-context dest_name | disconnect-dscp-label dscp-label_value| mtu | rohc-profile-name profile_name }

destination-context: Specify the intended destination context name. This value must be string of 1 to 79 characters in length.
disconnect-dscp-label: Configures the DSCP label to be present in the In Call Signalling packet based on which In Call Signalling and Media Flows will be disconnected. This value must be a Hexadecimal number between 0x0 and 0xF.
mtu: Configures maximum transmission unit. This value must be ranging from 100 to 2000. Default is 1500.
rohc-profile-name: Profile name of the ROHC compresser and decompressor. This value should be a string of 1 to 63.
Usage

Use this command to set the BCMCS group username and password for RADIUS access requests.

Example

```bash
bcmcs grpusername group_name bcmcs grppassword group_password
```
data-available-indicator

Enable sending Data Available Indicator extension in R-P Registration Reply.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

data-available-indicator

no data-available-indicator

no
Default: Disabled
Disable the sending of the Data Available Indicator extension in R-P Registration Reply.

**Usage**
Use this command to enable or disable the sending of the Data Available Indicator extension in R-P Registration Reply.

**Example**
Use the following command to enable sending the Data Available Indicator extension in R-P Registration Reply:

data-available-indicator

Use the following command to disable sending the Data Available Indicator extension in R-P Registration Reply:

no data-available-indicator
data-over-signaling

Enable the data-over-signaling marking feature for A10 packets.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
data-over-signaling
no data-over signaling
```

**no**
Default: Enabled
Disable the data-over signaling feature for A10 packets.

**Usage**
Use this command to enable or disable the data-over signaling feature for A10 packets.

**Important**: This is a customer-specific command.

**Example**

```
no data-over-signaling
```
default

Sets / Restores default value assigned for specified parameter.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
default { authentication | gre { checksum | checksum-verify | protocol-type | sequence-numbers } | inter-pdsn-handoff mobility-event-indicator | ip { local-port | source-violation { drop-limit | period | reneg-limit }} | lifetime | max-retransmissions | pf-monitor | policy { overload | service-option } | registration-accept handoff session-disconnect-in-progress | registration-deny { handoff connection-setup-record-absent | max-deny-reply-limit | new-call { connection-setup-record-absent | reverse-tunnel-unavailable } | session-already-active | session-already-closed | session-already-dormant | terminate-session-on-error | use-zero-gre-key | session-already-closed | terminate-session-on-error | registration-discard { bad-extension | gre-key-change } | registration-update wait-timeout | retransmission-timeout | service-option | setup-timeout }
```

`registration-update wait-timeout`

Sets the PDSN service to not wait before sending Registration-Update when PPP is terminated for an active RP session.

`authentication`

Sets/restores the authentication setting to their defaults which are as follows:
- allow-noauth disabled
- chap enabled with a priority of 1
- mschap enabled with a priority of 3
- msid-auth disabled
- pap enabled with a priority of 2

`gre { checksum | checksum-verify | protocol-type | sequence-numbers }`

`checksum`: Disables the introduction of the checksum field in outgoing GRE packets.
`checksum-verify`: Disables verification of the GRE checksum (if present) in incoming GRE packets.
`protocol-type`: Restores the GRE protocol type the default protocol-type any
`sequence-numbers`: Restores the GRE sequence number parameters to the default sequence-numbers enabled

`inter-pdsn-handoff mobility-event-indicator`

Disables support for the Mobile Event Indicator during inter-PDSN handoffs.
PDSN Service Configuration Mode Commands

**ip local-port**
Restores the ip local-port setting to its default value of 699.

**ip source-violation {drop-limit | period | reneg-limit}**
Sets the source violation parameters to the defaults or sets the defaults to the specified value as follows:

- **drop-limit**: Sets the number of source violations within a detection period before forcing a call disconnect to the default: 10.
- **period**: Sets the length of time, in seconds, for a source violation detection period to last to the default: 120 seconds.
- **reneg-limit**: Sets the number of source violations within a detection period before forcing a PPP renegotiation to the default: 5.

**lifetime**
Restores the lifetime setting to its default: 1800 seconds.

**max-retransmissions**
Restores the max-retransmissions setting to its default: 5.

**pcf-monitor**
Restores the PCF monitoring settings to the defaults.
Default interval: 900
Default num-retry: 5
Default timeout: 5

**policy { overload | service-option }**
Restores the policy overload and/or policy service-option setting to its default values as follows:

- overload disabled
- sequence-numbers enforced enabled

**registration-accept handoff session-disconnect-in-progress**
Resets the PDSN to deny registration requests when a handoff disconnect is still in progress.

**registration-deny { handoff connection-setup-record-absent | max-deny-reply-limit | new-call { connection-setup-record-absent | reverse-tunnel-unavailable } | session-already-active | session-already-closed | session-already-dormant | terminate-session-on-error | use-zero-gre-key**

**handoff connection-setup-record-absent**
- **connection-setup-record-absent**: Accept handoff R-P sessions that do not have an Airlink Connection Setup record in the RRQ Request.

**max-deny-reply-limit**: Resets the maximum number of retries of erroneous registration reply message from PCF for a session before PDSN terminates the session. to the default. Default is 3.

**new-call connection-setup-record-absent**: Configures the PDSN not to reject calls that do not have the PDSN connection setup record in the RRQ.

**new-call reverse-tunnel-unavailable**: Configures the PDSN not to reject calls if the GRE key for a user collides with that of another user.
session-already-active: <span class="emphasis">disables</span> the PDSN from denying RP renew and dereg requests for active R-P sessions.

session-already-closed: <span class="emphasis">disables</span> the PDSN from denying RP renew and dereg requests for absent R-P sessions.

session-already-dormant: <span class="emphasis">disables</span> the PDSN from denying RP renew and dereg requests for dormant R-P sessions.

terminate-session-on-error: Disables the PDSN from terminating a session if an erroneous registration request message is received for the session.

use-zero-gre-key: Configures the PDSN not to set the GRE key to zero (0) when denying a new R-P session.

registration-discard { bad-extension | gre-key-change }

bad-extension: Set the PDSN so that it does not immediately discard registration requests that have multiple vendor information elements of the same type.

gre-key-change: Sets the PDSN so that it does not discard Registration Requests that have a GRE key that is different than the one for the existing IMSI session.

handoff connection-setup-record-absent: Sets the PDSN so that it does not discard A11 Handoff requests that do not contain the Airlink Setup record.

registration-update wait-timeout

Sets the PDSN service to not wait before sending Registration-Update when PPP is terminated for an active RP session.

retransmission-timeout

Restores the retransmission-timeout setting to its default: 3 seconds.

service-option

Restores the service-option setting to its default list of service options as follows:

- 7: PCF specific
- 15: PCF specific
- 22: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS1 reverse)
- 23: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS2 reverse)
- 24: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS1 reverse)
- 25: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS2 reverse)
- 33: 3G High Speed Packet Data
- 59: PCF specific

setup-timeout

Restore the maximum amount of time allowed for setting up a session to the default of 60 seconds.

Usage

After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.
Example
The following command is used to return the lifetime parameter to its default value:

    default lifetime
default subscriber

Specifies the name of a subscriber profile configured within the same context as the PDSN service from which to base the handling of all other subscriber sessions handled by the PDSN service.

**Product**  
PDSN

**Privilege**  
Security Administrator, Administrator

**Syntax**

```plaintext
default subscriber profile_name

no default subscriber profile_name
```

- **profile_name**  
  Specifies the name of the configured subscriber profile. `profile_name` can be between 1 and 63 alpha and/or number characters and is case sensitive.

**Usage**

Each subscriber profile specifies “rules” such as permissions, PPP settings, and timeout values. By default, the PDSN service will use the information configured for the subscriber named default within the same context. This command allows for multiple PDSN services within the same context to apply different “rules” to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the `no default subscriber profile_name` command to delete the configured default subscriber.

**Example**

To configure the PDSN service to apply the rules configured for a subscriber named `user1` to every other subscriber session it processes, enter the following command:

```plaintext
default subscriber user1
```
dormant-transition

Configures the PDSN behavior to terminate A10 session, when the PDSN receives the A11-RRQ (Type 4) before the session for the original MN is established completely.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no | default] dormant-transition initial-session-setup
```

- **no**
  Terminates the A10 session, when PDSN receives the A11-RRQ (Type 4) before the original session established completely.

- **default**
  Keeps the A10 session live in case of A11-RRQ (Type 4) is received before the original session is established completely.

**Usage**

When the status of A10 session goes to dormant before the session for the original MN is established completely, the different MN may possibly send the A11-RRQ (Type 4) to the PDSN and PPP renegotiation may start.

This command is used to terminate the A10 session when the PDSN receives the A11-RRQ (Type 4) before the session for original MN is established completely.

**Example**

Following command is used to release the A10 session in case of receiving A11-RRQ (Type 4) before the original session is established completely:

```
no dormant-transition initial-session-setup
```


end

Exits the PDSN service configuration mode and returns to the Exec mode.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the PDSN service configuration mode and returns to the context configuration mode.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
fragment

It enables/disables fragmentation of PPP data.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

fragment ppp-data
[ no | default ] fragment ppp-data

no
Disables the fragmentation of ppp data.

default
Default enables ppp data fragmentation.

Usage
This command is to indicate to the RP module to NOT fragment PPP payloads being sent to the PCF, if the total packet size (PPP+GRE+IP) exceeds 1500 bytes. Disabling fragmentation may cause the sessmgr to perform outer IP fragmentation of the outgoing packet, if the resulting packet exceeds the MED MTU.
gre

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
gre { checksum | checksum-verify | flow control | ip-header-dscp value { all-control-packets | setup-packets-only } | flow-control-timeout { seconds | msec milliseconds } action { resume-session | disconnect-session } | protocol-type { any | byte-stream | ppp } | reorder-timeout milliseconds | sequence-mode { none | reorder } | segmentation | sequence-numbers | threegpp2-ext-header qos-marking }
```

```
no gre { checksum | checksum-verify | flow-control | ip-header-dscp | segmentation | sequence-numbers | threegpp2-ext-headers qos-marking }
```

```
default gre { checksum | checksum-verify | flow-control | ip-header-dscp | segmentation | sequence-mode | sequence-numbers | threegpp2-ext-headers qos-marking }
```

```
no
```

Disables the specified functionality.

```
default
```

Restores the specified parameter to its default setting.

```
checksum
```

Default: disabled

Enables the introduction of the checksum field in outgoing GRE packets.

```
checksum-verify
```

Default: disabled

Enables verification of the GRE checksum (if present) in incoming GRE packets.

```
ip-header-dscp value { all-control-packets | setup-packets-only }
```

Default: Disabled

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- **Value**: Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F.

- **All-control-packets**: Dictates that the DSCP marking is to be provided in all GRE control packets.
**setup-packets-only**: Dictates that the DSCP marking is to be provided only in GRE setup packets.

```plaintext
flow-control [action {disconnect-session | resume-session}] [timeout {seconds | msec milliseconds}]
```

Default: no gre flow-control

Enables 3GPP2 GRE flow control which causes the PDSN to send flow control enabled Normal Vendor Specific Extensions (NVSE) in A11 RRPs.

- **action**: Specifies the action to be taken when timeout is reached:
  - **disconnect-session**: (default): Ends the session and releases the call.
  - **resume-session**: Switches flow control to XON and resumes delivery of packets to the RAN.

- **timeout**: Sets the amount of time wait for an XON indicator from the RAN (after receiving an XOFF). Also sets the action to be taken if the timeout limit is reached.

Default: 10 seconds, disconnect-session

- **seconds**: Specifies the amount of time in seconds before the timeout is reached. **seconds** must be an integer from 1 through 1000.

- **msec milliseconds**: Specifies the amount of time in milliseconds before the timeout is reached. **milliseconds** must be an integer from 1 through 1000000.

```plaintext
protocol-type { any | byte-stream | ppp }
```

Specifies the protocol used for GRE encapsulation that is acceptable to

- **any**: Specifies that the PDSN service will accept GRE packets encapsulated using any protocol.

- **byte-stream**: Specifies that the PDSN service will accept GRE packets only encapsulated using byte stream. Using byte stream encapsulation, PPP packets are framed at different intervals and sent.

- **ppp**: Specifies that the PDSN service will accept GRE packets only encapsulated using the Point-to-Point Protocol (PPP). Using PPP encapsulation, PPP packets are framed at regular intervals and sent.

```plaintext
reorder-timeout
```

Default: 100

Configures max number of milliseconds to wait before processing reordered out-of-sequence GRE packets. **milliseconds** must be an integer from 0 through 5000.

```plaintext
segmentation
```

Default: disabled

Enables GRE Segmentation for the PDSN service.

```plaintext
sequence-mode { none | reorder }
```

Default: none

Configures handling of incoming out-of-sequence GRE packets.

- **none**: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.

- **reorder**: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:
  - The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
- The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

**sequence-numbers**

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.

**threegpp2-ext-headers qos-marking**

When threegpp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the PDSN will include the qos optional data attribute in the GRE 3gpp2 extension header.
The `no` keyword, enables qos-marking in the gre header based on the tos value in the header.

**Usage**

The `gre protocol-type` command can be used to prevent the PDSN service from servicing PCFs that use a specific form of encapsulation.
Use the `no gre sequence-numbers` command to disable the inclusion of GRE sequence numbers in the A10 data path.
The chassis is shipped from the factory with the authentication options set as follows:

- `protocol-type any`
- `sequence-numbers enabled`

**Example**

Use this command to configure the PDSN service to exclude byte stream encapsulated GRE traffic:

```
gre protocol-type ppp
```
inter-pdsn-handoff mobility-event-indicator

Configures the PDSN to support the Mobility Event Identifier (MEI) during inter-PDSN handoffs. The presence of the Mobility Event Indicator (MEI) and Access Network Identifier (ANID) elements in an A11 handoff request represents an Inter-PDSN handoff.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
inter-pdsn-handoff mobility-event-indicator
no inter-pdsn-handoff mobility-event-indicator

no
Disables support for the MEI during inter-PDSN handoffs.
```

**Usage**

Use this command to configure support for the MEI during inter-PDSN handoffs.

**Example**

Use the following command to enable support for the MEI during inter-PDSN handoffs:

```plaintext
inter-pdsn-handoff mobility-event-indicator
```
ip header-compression rohc

This command enters PDSN Service ROHC Configuration Mode. The ROHC configuration mode lets you configure ROHC parameters that PDSN conveys to the PCF in the initial A11 RRP message before PPP authentication. By default, ROHC is disabled for a PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

ip header-compression rohc
default ip header-compression rohc
no ip header-compression rohc

default
Set all PDSN Service ROHC Configuration Mode values back to the defaults and disable ROHC for this PDSN service.

no
Disable IP header compression for this PDSN Service.

Usage
Use this command to enter the PDSN Service ROHC Configuration Mode or disable ROHC for the current PDSN service.

Example
The following command enters PDSN Service ROHC Configuration Mode:

ip header-compression rohc

The following command disables ROHC for the current PDSN service and sets all of the values for commands in PDSN Service ROHC Configuration Mode back to their default settings:

default ip header-compression rohc
ip local-port

Configures the local User Datagram Protocol (UDP) port for the R-P interfaces’ IP socket.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
ip local-port number
```

*number*
Default: 699
Specifies the UDP port number.

*number* can be any integer value between 1 and 65535.

Usage

Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the PDSN.

**Important:** The UDP port setting on the PCF must match the local-port setting for the PDSN service on the system in order for the two devices to communicate.

Example

Use the following command to specify a UDP port of 3950 for the PDSN service to use to communicate with the PCF on the R-P interface:

```
ip local-port 3950
```
ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product
PDSN, PDIF

Privilege
Security Administrator, Administrator

Syntax

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num }
no ip source-violation clear-on-valid-packet
```

**clear-on-valid-packet**
Default: disabled
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

**drop-limit num**
Default: 10
Sets the number of allowed source violations within a detection period before forcing a call disconnect. If `num` is not specified, the value is set to the default. `num` can be any integer value from 1 to 1000000.

**period secs**
Default: 120
The length of time, in seconds, for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If `secs` is not specified, the value is set to the default. `secs` can be any integer value from 1 to 1000000.

**reneg-limit num**
Default: 5
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If `num` is not specified, the value is set to the default. `num` can be any integer value from 1 to 1000000.

Usage
This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDIFs PDSNs a number of times during a handoff scenario. This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.

If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.

If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by 1. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

---

**Example**
The following command sets the drop limit to 15 and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```
lifetime

Specifies the time that an A10 connection can exist before its registration is considered expired.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
lifetime time
no lifetime
```

The `no lifetime` command specifies that an A10 connection can exist for an infinite amount of time.

**time**

Default: 1800

Specifies the time that an A10 connection can exist before its registration is considered expired.

- `time` is measured in seconds and can be configured to any integer value between 1 and 65534.

**Usage**

Set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, their connection will be terminated automatically.

Use the `no lifetime` command to delete a previously configured lifetime setting. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the `default lifetime` command.

**Example**

The following command specifies a time of 3600 seconds (1 hour) for subscriber sessions on this PDSN service:

```plaintext
lifetime 3600
```
max-retransmissions

Configures the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
max-retransmissions count
```

count

Specifies the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

count can be configured to any integer value between 1 and 1,000,000.

Usage
If the value configured for the max-retransmissions is reached the call will be dropped.
The chassis is shipped from the factory with the Internet maximum number of retransmissions set to 5.

Example
The following command configures the maximum number of retransmissions for the PDSN service to 3:

```
max-retransmissions 3
```
mobile-ip foreign-agent context

For Mobile IP support, specifies the context in which the FA service(s) are configured.

<table>
<thead>
<tr>
<th>Product</th>
<th>PDSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax**

```
mobile-ip foreign-agent context context_name [fa-service name]
no mobile-ip foreign-agent context context_name [fa-service name]
```

**context_name**

Specifies the name of the previously configured context that facilitates the FA service(s).

context_name must be between 1 and 79 alpha or numeric characters and is case sensitive.

**[fa-service name]**

This optional keyword allows you to link the PDSN service to a particular FA service in the specified context. name is the name of the FA service to link to.

**Usage**

FA services on the system can be configured either in the same or different contexts from those facilitating PDSN services. When they are configured in separate contexts, this command configured with a PDSN service instructs the PDSN service to route traffic to the context facilitating the FA service.

Use the `no mobile-ip foreign-agent context` to delete a previously configured destination context.

**Example**

The following command instructs the PDSN service to use the context named FA-destination for FA functionality:

```
mobile-ip foreign-agent context fa-destination
```
**msid length**

Specifies the allowed configurable Mobile Station IDentifier (MSID) length.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default ] msid length [ min min_length ] max max_length
```

- **default**
  Specifies the default length of MSID (10 to 15) as per standard.

- **min min_length**
  Specifies the minimum length for MSID.
  *min_length* is any Integer value between 10 to 15, but should be less than *max_length* specified with **max**.

- **max max_length**
  Specifies the maximum length for MSID.
  *max_length* is any Integer value between 10 to 15, but should be more than *min_length* specified with **min**.

**Usage**
MSID length can be configured either in the standard length or different customized length form. This command is used to specify the allowed length of MSID.

**Example**
The following command specifies an MSID length between 12 and 15:

```
msid length min 12 max 15
```
nai-construction

Specifies a domain alias that will be used to represent the context which the PDSN service should use for AAA functionality.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
nai-construction domain alias
no nai-construction domain
```

**domain alias**

alias represents the “domain” name that you would like to associate with the context in which AAA functionality is configured. alias can be between 1 and 79 alpha and/or numeric characters and is case-sensitive.

Usage

Enabling NAI will be constructed for the subscriber in the event that their mobile station (MS) does not negotiate CHAP, PAP, or MSCHAP. If this option is selected, no further attempts will be made to authenticate the user. Instead, the constructed NAI will be used for accounting purposes.

The context specified by this command would be used to provide the communication with the RADIUS accounting server.

Use the `no nai-constructed domain` command to deleted a configured alias.

**Important:** This command should only be used if the PDSN service is configured to allow no authentication using the authentication allow-noauth command.

Additionally, the `aaa constructed-nai` command in the Context Configuration mode can be used to configure a password for constructed NAI.

Example

The following command configured a domain alias of aaa_context for the PDSN service to use when an NAI is constructed for a subscriber session:

```
nai-construction domain aaa_context
```
new-call conflict

Enable or disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
new-call conflict terminate-session-old-pcf [no | default] new-call conflict terminate-session-old-pcf
```

**no**

Disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

**default**

Enable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Usage
This configuration supports to enable or disable to send A11-RUPD to current PCF, when the system receives the A11-RRQ(Type1) from new PCF during the session exists.
If the configuration is **no new-call conflict terminate-session-old-pcf** system will not send registration update to old PCF on receiving a new call (A11-RRQ(Type1)) request for an existing active/dormant session. The default behavior is to send registration updates.

Example
The following command configured a system to send a registration update on receiving an A11-RRQ (Type 1) request for an existing active/dormant session:

```
new-call conflict terminate-session-old-pcf
```
pcf-monitor

When this is enabled, the PDSN monitors all the PCFs that have sessions associated with it. The PDSN stops monitoring a PCF if it is determined to be down. Once a PCF is determined to be down, the PDSN tears down all sessions that correspond to the PCF and generates AAA Accounting Stop messages. All the PCFs that are connected to the PDSN service are monitored.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
pcf-monitor [ interval seconds | max-inactivity-time seconds | num-retry num | timeout seconds ]
no pcf-monitor
```

**pcf-monitor**

Entering the command with no keywords enables the PCF monitoring function with all parameters set to the defaults.

**no**

Disables the pcf monitoring function.

**interval seconds**

Default: 900 seconds
Sets the amount of time to wait between ping request messages.
seconds must be an integer in the range from 60 through 3600.

**max-inactivity-time seconds**

Default: 120 seconds
The maximum amount of time (seconds) with no A10 traffic from a PCF before the ICMP-ping mechanism is triggered.
seconds must be an integer from 1 through 3600.

**num-retry num**

Default: 5
Sets the number of times that the PDSN retries to ping the PCF. When num-retry for a given PCF has been exhausted with no response, sessions that correspond to the non-responsive PCF are terminated and Accounting Stop records for each terminated session are generated.
num must be an integer in the range from 0 through 100.

**timeout seconds**

Default: 5 seconds
The amount of time to wait for a response before retrying.
seconds must be in the range from 1 through 10.

Usage
Use this command to enable the PDSN service to monitor the PCFs that have sessions associated with the PDSN service.

Example
The following command enables PCF monitoring with parameters set to the defaults:

```
pcf-monitoring
```

The following command enables PCF monitoring and sets the timeout to 10 seconds:

```
pcf-monitor timeout 10
```

The following command disables pcf-monitoring:

```
no pcf-monitor
```
pcf-session-id-change restart-ppp

This feature manages current session and PPP renegotiation on GRE-key change without any change in PCF/PANID/CANID. This command disables or enables the PPP renegotiation restart on receiving an RP registration request from the current PCF with GRE key (PCF session Id) change. With this command the PDSN aborts and restarts the call causing PPP renegotiation.

This is enabled by default.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

[no | default] pcf-session-id-change restart-ppp

no
Disables the pcf-session-id-change restart-ppp function.
With this option PDSN does not restart the PPP renegotiation on GRE key change from current PCF in an RP registration request, unless it indicates change in PCF/PANID/CANID.

default
Set the pcf-session-id-change function to the default state on enabled.

Usage
GRE key (PCF session ID) is sued to identify the data packet for a session and is negotiated through the A11 signaling messages between PCF and PDSN. By default PDSN aborts and restart the PPP renegotiation on receipt of any RP registration request with change in GRE key or PCF session Id.
With use of no pcf-session-id-change restart-ppp command PDSN is configured to disable the restart of call or PPP renegotiation on receipt of any RP registration request with changed GRE key, unless it has any PCF/ANID/CANID change. PDSN silently switches the GRE key for the session, retaining the existing PPP session.

Example
The following command disables the PPP renegotiation restart action on receipt of any RP RRQ with changed GRE key from same PCF/PANID/CANID.

no pcf-session-id-change restart-ppp
**pdsn type0-tft attempt-inner-match**

Configures a type0 traffic flow template (tft) to a type1 traffic flow template.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
pdsn type0-tft attempt-inner-match
no pdsn type0-tft attempt-inner-match
```

**Usage**
This CLI is used make PDSN match inner IP packets for an AIMS call. When enabled, the PDSN tries to match a type-0 tft to match both outer and inner packet, so that MN can use a Type-0 filter for HoA traffic which are tunneled.
This is disabled by default.

**Example**
The following command enables type0 tft:

```
pdsn type0-tft attempt-inner-match
```
peer-pcf

Confogures settings for any PCF that has a connection with this PDSN.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
peer-pcf ip_address bcmcs_framing { hdlc-like | segment-based }
```

- `ip_address`
  - `ip_address` must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.

- `bcmcs_framing { hdlc-like | segment-based }
  - Specifies the type of bcmcs_framing to use for this PCF connection.
    - `hdlc-like`: applies HDLC-like framing for all BCMCS flows
    - `segment-based`: applies segment-based framing for all BCMCS flows

**Usage**

Use this command to configure the settings for any PCF that is connected to this PDSN. You can also specify bcmcs framing settings to use for the connection.

**Example**

The following command configures the peer-pcf for an IP address of 131.2.3.4:

```
peer-pcf 131.2.3.4
```
policy

Configures PDSN service policies.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

policy overload { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] } | { reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }  

policy msid-match msid_with_wildcards { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] }  

policy pcf-zone-match zone_number { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] }  

no policy { msid-match msid_with_wildcards | overload [ redirect address ] | pcf-zone-match zone_number | rrq mei-from-current-pcf (suppress-ppp-restart) | service-option | unknown-cvse enforce }  

Deletes a previously set policy or removes a redirect IP address.

overload: This keyword without any options deletes the complete overload policy from the PDSN service.

overload redirect address [ address2 ... address16 ]; deletes up to 16 IP addresses from the overload redirect policy. The IP addresses must be expressed in IP v4 dotted decimal notation.

rrq mei-from-current-pcf suppress-ppp-restart: suppresses the PPP restart, when RRQ containing MEI comes from the current PCF. This is disabled by default.

service-option: Resets the PDSN service to accept calls that do not contain the service option(s) configured using the service option command.

unknown-cvse enforce: When unknown-cvse policy is enforced, PDSN will deny RRQs with unknown CVSEs (unknown vendor id, unknown app type or unknown app subtype) with an error code. When disabled, PDSN will process the CVSE like an NVSE. If an unknown vendor-id, app-type or app-subtype is encountered during the processing of a CVSE, the entire CVSE will be ignored and rest of the RRQ will be processed.

policy overload { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] } | { reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }  

Specifies how a PDSN service should handle an overload condition.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.
address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values. weight weight_num When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.

reject: This option will cause any overload traffic to be rejected. The PDSN will send an A11 Registration Reply Code of 82H (insufficient resources).

use-reject-code admin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code insufficient resources. This is the default behavior.

use-reject-code insufficient-resources: When this keyword is specified and traffic is rejected, the error code insufficient resources is returned instead of the error code admin prohibited.

policy msid-match msid_with_wildcards { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] }

Specifies how a PDSN service should handle an incoming call that matches a list of wildcard MSIDs.

msid_with_wildcards: An MSID in which up to 16 digits have been replaced with the wildcard ‘$’. This defines the list of possible matches for incoming calls.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

direct: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values. weight weight_num When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.

policy pcf-zone-match zone_number { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] }

Specifies how a PDSN service should handle an incoming call that matches a predefined zone number.
zone_number: An integer between 1 and 32 that defines the zone incoming calls must match for redirection.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values. weight weight_num When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.
Usage
Policies can be implemented to dictate PDSN service behavior for various conditions such as overloading. The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system. The system automatically invokes the overload policy when an on-line software upgrade is started.
Use the no policy { overload|service-option } command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the default policy command.
The chassis is shipped from the factory with the policy options set as follows:
- overload disabled
- sequence-numbers enforced enabled

⚠️ Caution: Incorrect configuration of the policy msid-match and policy pcf-zone-match keywords could result in sessions failing to be established. For example, if PDSN1 is configured to redirect sessions to PDSN2 while PDSN2 is configured to redirect sessions to PDSN1, a loop is created in which all sessions would fail to be connected. In addition, sessions will not be established if the PDSN to which the sessions are being redirected is unavailable.

Example
The following command configures the PDSN service to redirect traffic to two different destinations with weights of 1 and 10 respectively:

```
  policy overload redirect 192.168.1.100 weight 1 192.168.1.200 weight 10
```
Sets PPP tunneling parameters for subscribers in the current PDSN service.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ppp { tunnel-context context_name | tunnel-type { 12tp | 12tp-secure | none } }
```

```plaintext
no ppp tunnel-context
```

- **no**
  Clears the configured tunnel context entry.

- **tunnel-context context_name**
  The name of the context that has a LAC service configured to handle all tunnels from this PDSN service.

- **tunnel-type { 12tp | 12tp-secure | none }**
  - **12tp**: Force all subscriber sessions in this PDSN service to use L2TP tunneling.
  - **12tp-secure**: Force all subscriber sessions in this PDSN service to use L2TP tunneling and use IPSEC to ensure a secure connection.
  - **none**: Do not force L2TP tunneling. This is the default.

**Important**: If the context specified by the `ppp tunnel-context context_name` command does not have a LAC service configured and `tunnel-type` is set to `12tp` or `12tp-secure`, the call is rejected.

**Important**: If the PPP tunnel context has not been set or has been cleared with the `no ppp tunnel-context` command and `tunnel-type` is set to `12tp` or `12tp-secure`, the context where the current PDSN service resides is used. If that context does not have a LAC service configured the call is rejected.

**Usage**

Use this command to enable or disable forced L2TP tunneling for all subscribers using this PDSN service. Also use this command to define which context defines the L2TP tunneling parameters.

**Example**

To set the tunnel context to the context named `context1` and enable forced L2TP tunneling, use the following commands;

```plaintext
ppp tunnel-context context1 ppp tunnel-type 12tp
```

To enable forced L2TP tunneling with IPSEC security, use the following commands;
To disable forced tunneling, use the following command:

```
ppp tunnel-type none
```

To clear the setting for the tunnel context, use the following command:

```
no ppp tunnel-context
```
qos-profile-id-mapping

This command creates the customized QoS profile identifier to QoS mapping for IMS authorization support through a Ty interface at the PDSN service level.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
qos-profile-id-mapping profile-id id_num { description desc | downlink-bw dl_bw | drop-rate drop_percentage | latency latency_duration | qos-class {class-A | class-B | class-C | class-D | class-E | class-F } uplink-bw ul_bw }+
```

```
[ default | no ] qos-profile-id-mapping profile-id id_num
```

```
default
Configures the specified QoS profile ID for QoS mapping with default values in this PDSN service.
```

```
no
Removes the configured QoS profile ID mapping in this PDSN service.
```

```
profile-id id_num
Specifies the profile identifier for QoS parameters to be used as the customized profile ID or modifies the QoS parameters in a profile ID (id_num) coming from RAN.
id_num must be an integer between 0 and 65535.
```

```
description desc
Specifies the user defined description for profile identifier.
desc must be an alpha and/or numeric string between 1 and 32 characters.
```

```
downlink-bw dl_bw
Default: 32
Specifies the downlink (towards the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.
dl_bw must be an integer value between 0 and 100000.
```

```
drop-rate drop_percentage
Default: 0
Specifies the permitted packet drop rate in percentage for traffic flow to this QoS profile.
drop_percentage must be an integer value between 0 and 100.
```

```
latency latency_duration
Default: 1000
Specifies the permitted latency duration in milli-seconds for this QoS profile.
latency_duration must be an integer value between 0 and 1000.
```
**qos-profile-id-mapping**

```plaintext
qos-class {class-A | class-B | class-C | class-D | class-E | class-F }
```

Default: Class-C

Specifies the type of QoS class associated with this QoS profile
class-A: Specifies the A type of QoS class.
class-B: Specifies the B type of QoS class.
class-C: Specifies the C type of QoS class.
class-D: Specifies the D type of QoS class.
class-E: Specifies the E type of QoS class.
class-F: Specifies the F type of QoS class.

```plaintext
uplink-bw ul_bw
```

Default: 32

Specifies the uplink (from the MN) data traffic bandwidth in kilo-bits per second for this QoS profile. `ul_bw` must be an integer value between 0 and 100000.

More than one of the above keywords can be entered within a single command.

**Usage**

Use this command to define the values associated with the profile ID on the PDSN. This profile ID is used during the mapping to and from the authorized QoS to the QoS parameters for the A10 link. This mapping is required because the PDSN only knows the profile IDs and not the actual configured values for the profile ID in the RAN. Also this configuration allows the use of custom profile IDs for the subscribers. If no values are defined with a QoS profile ID, the values from matching QoS profile ID from RAN will be applicable to the subscriber traffic.

**Example**

The following command sets the downlink bandwidth to 32 kbps, latency duration as 1000 ms, uplink bandwidth to 32 kbps, and QoS class to Class-C for the QoS profile ID 11 in a PDSN service:

```
default qos-profile-id-mapping profile-id 11
```
qos update

Use this command to set QoS update parameters for policy mismatches or wait timeouts.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
qos-update [ policy-mismatch | wait-timeout seconds action [ drop-packets | disconnect-session | downgrade-to-best-effort ] ]
```

**policy-mismatch**
PDSN raises a TFT violation if there is a QoS policy mismatch.

**wait-timeout action [ drop-packets | disconnect-session | downgrade-to-best-effort ]**
Sets the wait time for A11 RRQ for QoS changes. `seconds` must be an integer from 1 through 1000.

- **action**: configures the action on the wait-timeout
  - **disconnect-session**: Drops the call if the A11 RRQ has not been received for the QoS update. This includes all of the IP flows for the session.
  - **downgrade-to-best-effort**: Drops packets if the A11 RRQ has not been received for the QoS update. Sends the forward traffic over best effort (flow FF or FE if available).
  - **drop-packets**: Drops packets if the A11 RRQ has not been received for the QoS update.

Usage
This command provides a PDSN service level configurable to configure an action, if the PCF ignores the QoS Update request from PDSN. It sets the amount of time to wait and the action to take, if no RRQ is received before the timeout. The action can be to drop packets for the flow, disconnect the session or to downgrade to best effort.

Example

```
qos-update policy mismatch
```

The following command sets `wait-timeout` to 60 seconds and invokes `downgrade-to-best-effort` if the A11 RRQ has not been received for the QoS update:

```
qos-update wait-timeout 60 action downgrade-to-best-effort
```
registration-accept

When the PDSN is tearing down a session and the MN moves over to a new PCF and initiates a new session, the PDSN by default does not accept the handoff until it tears down the old session. This command allows the PDSN to accept registration requests when a handoff disconnect is in progress.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

- registration-accept handoff session-disconnect-in-progress
- no registration-accept handoff session-disconnect-in-progress

**Usage**
Use this command to allow the PDSN service to accept registration requests when a handoff disconnect is still in progress.

**Example**

registration-accept handoff session-disconnect-in-progress
registration-ack-deny terminate-session-on-error

Configure the PDSN service to terminate an A11 session when a Registration ACK received from the PCF has an error status.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
registration-ack-deny terminate-session-on-error
no registration-ack-deny terminate-session-on-error
```

**Usage**
Use this command to enable the PDSN service to terminate A11 sessions on a Registration ACK error from the PCF.

**Example**
Use the following command to enable this functionality in the PDSN:

```
registration-ack-deny terminate-session-on-error
```
registration-deny

Configures parameters related to registration rejection.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
registration-deny { handoff connection-setup-record-absent [ use-deny-code { poorly-formed-request | reason-unspecified } | max-deny-reply-limit num | mismatched-coa-source-address | new-call { connection-setup-record-absent | reverse-tunnel-unavailable } | session-already-active | session-already-closed | session-already-dormant | terminate-session-on-error | use-zero-gre-key

no registration-deny { handoff connection-setup-record-absent | max-deny-reply-limit | mismatched-coa-source-address | new-call { connection-setup-record-absent | reverse-tunnel-unavailable } | session-already-active | session-already-closed | session-already-dormant | terminate-session-on-error | use-zero-gre-key
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the specified option.</td>
</tr>
<tr>
<td>handoff</td>
<td>This command configures the handoff behavior.</td>
</tr>
<tr>
<td>connection-setup-record-absent</td>
<td>When enabled the PDSN denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default PDSN behavior is to accept such requests.</td>
</tr>
<tr>
<td>use-deny-code</td>
<td>Sets the specified Registration Deny Code when denying a handoff because of a missing connection setup record.</td>
</tr>
<tr>
<td>poorly-formed-request</td>
<td></td>
</tr>
<tr>
<td>reason-unspecified</td>
<td></td>
</tr>
<tr>
<td>max-deny-reply-limit num</td>
<td>Configures max number of retries of erroneous registration request message from PCF for a session before PDSN terminates the session. num can be from 1 to 10.</td>
</tr>
<tr>
<td>mismatched-coa-source-address</td>
<td>Denies RP requests which have a care-of-address field that is different from the request source address.</td>
</tr>
<tr>
<td>new-call</td>
<td></td>
</tr>
<tr>
<td>connection-setup-record-absent</td>
<td></td>
</tr>
<tr>
<td>reverse-tunnel-unavailable</td>
<td></td>
</tr>
<tr>
<td>session-already-active</td>
<td></td>
</tr>
<tr>
<td>session-already-closed</td>
<td></td>
</tr>
<tr>
<td>session-already-dormant</td>
<td></td>
</tr>
<tr>
<td>terminate-session-on-error</td>
<td></td>
</tr>
<tr>
<td>use-zero-gre-key</td>
<td></td>
</tr>
</tbody>
</table>

**max-deny-reply-limit num**

Default: 3

Configures max number of retries of erroneous registration request message from PCF for a session before PDSN terminates the session. num can be from 1 to 10.

**mismatched-coa-source-address**

Default: disabled

Denies RP requests which have a care-of-address field that is different from the request source address.
PDSN Service Configuration Mode Commands

**registration-deny**

- new-call { connection-setup-record-absent [ use-deny-code { poorly-formed-request | reason-unspecified } | reverse-tunnel-unavailable ] }

  **connection-setup-record-absent**: Configures the PDSN to reject calls that do not have the airlink connection setup record in the RRQ.
  **use-deny-code { poorly-formed-request | reason-unspecified }**: When rejecting calls that do not have the airlink setup record, use the specified deny code.
  **reverse-tunnel-unavailable**: Configures the PDSN to reject calls if the GRE key for a user collides with that of another user.

- **session-already-active**
  PDSN denies Registration requests for sessions that are already active with the error code “poorly formed request”.

- **session-already-closed**
  PDSN denies RP renew and dereg requests with error code 0x8E for absent R-P sessions.

- **session-already-dormant**
  PDSN denies Registration requests for sessions that are already dormant with the error code “poorly formed request”.

- **terminate-session-on-error**
  Default: Disabled.
  Configures PDSN to terminate session if erroneous registration request message is received for the session.

- **use-zero-gre-key**
  Configures the PDSN to set the GRE key to zero (0) when denying a new R-P session.

**Usage**

Use this command to configure parameters relating to the rejection of registration requests.

**Example**

To reject calls that do not have the airlink setup record in the RRQ, enter the following command:

```
registration-deny new-call connection-setup-record-absent
```

To reject calls if the GRE key collides with that of another user, enter the following command:

```
registration-deny new-call reverse-tunnel-unavailable
```

To set the GRE key to 0 (zero) when a new R-P session is denied, enter the following command:

```
registration-deny new-call use-zero-gre-key
```
registration-discard

Configures the PDSN service to discard any Registration Request message containing multiple information elements of the same type or a different GRE key for existing IMSI session.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

registration-discard { bad-extension | gre-key-change | handoff connection-setup-record-absent }

no registration-discard { bad-extension | gre-key-change | handoff connection-setup-record-absent }

no
Disables the discarding of Registration request messages containing multiple information elements or different GRE keys.

bad-extension
Default: Disabled
Configures the PDSN to discard Registration Request message containing multiple information elements of same type.

gre-key-change
Default: Disabled
Configures PDSN to discard Registration Request message containing different GRE key for existing IMSI session. Default is disable

handoff connection-setup-record-absent
Default: Disabled
When enabled, discards A11 Handoff requests that do not contain the Airlink Setup record.

Usage
Use this command to configure the PDSN service to discard and Registration Requests that contain multiple information elements of the same type or discard Registration Requests that contain GRE keys that have different GRE keys for the existing IMSI session.

Example
To configure the PDSN service to discard of Registration Requests that have multiple information elements of the same type, enter the following command:

registration-discard bad-extension
To configure the PDSN service to discard registration Requests that contain a GRE key that is different than the existing one for the existing IMSI session, enter the following command:

```
registration-discard gre-key-change
```
registration-update

Configures registration update related parameters for the PDSN.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
registration-update { pdsn-code-nvse | wait-timeout secs }
```

```
no registration-update { pdsn-code-nvse | wait-timeout secs }
```

**no**
If this option is used with the `pdn-code-nvse` keyword, then pdsn-code-nvse configuration is disabled.
If this option is used with the `wait-timeout` keyword, a separate A11 timer is not used. The PDSN waits
for the ppp retransmit-timeout and then sends the A11 Update. If a value is provided, then the "ppp
retransmit-timeout" is ignored and a separate A11 timeout is started immediately upon sending the LCP
Term-Ack. The A11 Update is then sent when the timer expires.
A value of 0 sends the A11 Update immediately after sending the LCP Term-Ack.

**pdn-code-nvse**
Adds the PDSN code NVSE in all A11 registration update messages.

**secs**
The number of seconds to wait. `secs` must be an integer in the range from 0 through 16.

**wait-timeout**
After the Mobile Node terminates a PPP session between the PDSN and the Mobile Node, the PDSN service
waits for the specified time period to receive an A11 RRQ from the PCF before it sends out a Registration-
Update to clear the Session from the PCF.

**Usage**
Use this command to configure registration update related
The `wait-timeout` keyword configures the PDSN to wait the specified amount of time before sending
out a Registration-Update to clear the Session from the PCF.

**Example**
Use the following command to set the registration wait-timeout to 16 seconds:

```
registration-update wait-timeout 16
```
retransmission-timeout

Configures the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
retransmission-timeout time
no retransmission-timeout
```

time

Specifies the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.

time is measured in seconds and can be configured to any integer value between 1 and 1,000,000.

Usage

Use the retransmission timeout command in conjunction with the max-retransmissions command in order to configure the PDSN services behavior when it does not receive a response from a particular PCF.

Use the no retransmission-timeout command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the default retransmission-timeout command.

The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example

The following command configures a retransmission timeout value of 5 seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:

```
no retransmission-timeout
```
sdb-indication

Configures parameters pertaining to Short Data Burst (SDB) functionality.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

sdb-indication { echo-request | server-address ipaddress/mask packet-length-range min min_range max max_range }

no sdb-indication { echo-request | server-address ipaddress/mask }

no
Disables short-databurst indication.

echo-request
Default: Disabled
Enables the inclusion of the SDB indicator in the LCP Echo Request message(s).

server-address ipaddress/mask
Configures the IP address of the PTT server.
ipaddress is the IP address expressed in dotted decimal notation.
mask is the number of mask bits.

packet-length-range min min_range max max_range
Configures the packet length associated with the specified server.
min min_range configures the minimum packet length as an integer value between 1 and 65535.
max max_range configures the maximum packet length as an integer value between 1 and 65535.

Usage
This command controls the use of Short Data Burst functionality between the PDSN, PCF, and Push-to-Talk (PTT) servers.

Important: This command is for use with a customer-specific implementation and requires a valid Short Data Burst feature-use license to be installed.

Example
The following command configures a PTT server address of 192.168.1.200 with a mask of 16, a minimum packet size of 200, and a maximum packet size of 400:
sdb-indication server-address 192.168.1.200/16 packet-length-range min 200 max 400
service-option

If the service option policy is enabled, this command specifies the service options supported by the PDSN service.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
service-option number
no service-option number
```

`number`
Default: 7, 15, 22, 24, 25, 33, 59, 67
Specifies a specific Service Option (SO) number that this PDSN service is allowed to support.
number can be configured to any integer value between 1 and 1000.

**Usage**
Use the service option command in conjunction with the policy service option enforce command to configure specific SO numbers that are supported. If a particular SO number is not configured, then any subscriber session received with that SO number will be rejected and an A11 Registration Reply Code of 86 (poorly formed request) will be sent.
By default, PDSN services are configured to support the following service option numbers:
- 7: PCF specific
- 15: PCF specific
- 22: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS1 reverse)
- 23: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS2 reverse)
- 24: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS1 reverse)
- 25: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS2 reverse)
- 33: 3G High Speed Packet Data
- 59: High Rate Packet Data
- 67: RP A10 connection

**Important:** Option 67 is used for auxiliary connections for Rev-A calls. PPP encapsulation of data packets does not flow over this service option connection. ROHC can be performed without PPP for this service option.

Use the `no service-option number` command to delete a previously configured service option. If after deleting the service option setting you desire to return the service option parameter to its default setting, use the `default service-option` command.
Example
The following command enables a service option of 12:

    service-option 12

The following command disables the default service option 59:

    no service-option 59
setup-timeout

The maximum amount of time allowed for session setup.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
setup-timeout seconds
```

*seconds*
Default: 60 seconds
The maximum amount of time, in seconds, to allow for setup of a session. *seconds* must be an integer from 1 through 1000000

**Usage**
Use this command to set the maximum amount of time allowed for setting up a session.

**Example**
Use the following command to set the maximum time allowed for setting up a session to 300 seconds:
```
setup-timeout 300
```
simple-ip allow

This command is used to disable or re-enable Simple-IP sessions from making a connection before authorization takes place.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no|default] simple-ip allow
```

**no**
When a session attempts PPP authentication, it is assumed that it is a Simple-IP session and it is disconnected before the user is authenticated (RADIUS or local authentication). Also, if `allow-noauth` is enabled and PPP authentication is not performed, after IPCP the session is disconnected if it is discovered that it is a Simple-IP session.

**default**
Reset this command to allow Simple-IP sessions to connect.

**Usage**
Use this command to prevent Simple-IP sessions from connecting to a PDSN service.

**Example**
The following command configures the PDSN service so that it will reject any Simple-IP sessions:

```
no simple-ip allow
```

The following command configures the PDSN service to allow Simple-IP sessions:

```
simple-ip allow
```
spi

Configures the security parameter index (SPI) between the PDSN service and the PCF. This command also configures the redirection of call based on PCF zone.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
spi remote-address { pcf_ip_address | ip_addr_mask_combo } spi-number number { encrypted secret enc_secret | secret secret } [ description string ] [ hash-algorithm { md5 | rfc2002-md5 } ] [ replay-protection { nonce | timestamp } ] [ timestamp-tolerance tolerance ] [ zone zone_id ]
```

```
no spi remote-address pcf_ip_address spi-number number
```

**remote-address**

- **pcf_ip_address**: Specifies the IP address of the PCF. `pcf_ip_address` is an IP address expressed in IP v4 dotted decimal notation.
- **ip_addr_mask_combo**: Specifies the IP address of the PCF and specifies the IP address network mask bits. `ip_addr_mask_combo` must be specified using the form ‘IP Address/Mask Bits’ where the IP address must either be an IPv4 address expressed in dotted decimal notation or an IPv6 address expressed in colon notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

**spi-number**

Specifies the SPI (number) which indicates a security context between the PCF and the PDSN in accordance with IOS 4.1 and RFC 2002. number can be configured to any integer value between 256 and 4294967295.

**encrypted secret**

- **enc_secret**: Specifies the encrypted shared key (enc_secret) between the PCF and the PDSN service. `enc_secret` must be between 1 and 254 alpha and/or numeric characters and is case sensitive.
- **secret**: Specifies the shared key (secret) between the PCF and the PDSN services. `secret` must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

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

**description**

This is a description for the SPI. `string` must be an alpha and or numeric string of from 1 through 31 characters.
hash-algorithm { md5 | rfc2002-md5 }
Default: md5
Specifies the hash-algorithm used between the PDSN service and the PCF.
md5: Configures the hash-algorithm to implement MD5 per RFC 1321.
rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

replay-protection { nonce | timestamp }
Default: timestamp
Specifies the replay-protection scheme that should be implemented by the PDSN service.
nonce: Configures replay protection to be implemented using NONCE per RFC 2002.
timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance tolerance
Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.
tolerance is measured in seconds and can be configured to any integer value between 0 and 65535.

zone zone_id
Specifies the different PCF zones to configure in PDSN service. Mapping of a zone-number to a set of PDSNs can be done per PDSN service basis.
zone_id must be an integer value between 1 and 32. A maximum of 32 PCF zones can be configured for a PDSN service.

Usage
An SPI is a security mechanism configured and shared by the PCF and the PDSN service. Please refer to IOS 4.1 and RFC 2002 for additional information.
Multiple SPIs can be configured if the PDSN service is communicating with multiple PCFs.

Important: The SPI configuration on the PCF must match the SPI configuration for the PDSN service on the system in order for the two devices to communicate properly.

Use the no version of this command to delete a previously configured SPI.
This command used with zone zone_id redirects all calls on the basis of PCF zone to the specific PDSN on the basis of parameters configured at policy pcf-zone-match command.

Example
The following command configures the PDSN service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the PDSN service is q397F65.

spi remote-address 192.168.0.2 spi-number 256 secret q397F65

The following command deletes the configured SPI of 400 for an PCF with an IP address of 172.100.3.200:

no spi remote-address 172.100.3.200 spi-number 400
The following command creates the configured SPI of 400 for an PCF with an IP address of 172.100.3.200 and zone id as 11:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```
spi zone

Configures the security parameter index (SPI) between the PDSN service and the PCF with mapping between a zone number to a set of PDSNs per PDSN service to redirect call on the basis of PCF zone.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
spi zone zone_id

no spi zone zone_id
```

```
zone zone_id
Default: 60
```

Specifies the different PCF zones to configure in PDSN service. Mapping of a zone-number to a set of PDSNs can be done per PDSN service basis.

```
zone_id must be an integer value between 1 and 32. A maximum of 32 PCF zones can be configured for a PDSN service.
```

Usage

An SPI is a security mechanism configured and shared by the PCF and the PDSN service. Please refer to IOS 4.1 and RFC 2002 for additional information.

Multiple SPIs can be configured if the PDSN service is communicating with multiple PCFs.

This PCF zone option is used for call redirection on the basis of PCF zone. When a new call arrives the PDSN, it checks whether the PCF, from which the call arrived, belongs to a particular zone. If

```
Important: The SPI configuration on the PCF must match the SPI configuration for the PDSN service on the system in order for the two devices to communicate properly.
```

Use the no version of this command to delete a previously configured SPI.

Example

The following command configures the PDSN service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the PDSN service is q397F65.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command deletes the configured SPI of 400 for an PCF with an IP address of 172.100.3.200:

```
no spi remote-address 172.100.3.200 spi-number 400
```
threshold a11-rrp-failure

Set an alarm or alert based on the number of A11 Registration Response failures for the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
threshold a11-rrp-failure high_thresh [ clear low_thresh ]
no threshold a11-rrp-failure
```

```
no
Delete the alert or alarm.
```

```
high_thresh
Default: 0
The high threshold number of A11 Registration Response failures that must be met or exceeded within the
polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.
```

```
clear low_thresh
Default: 0
The low threshold number of A11 Registration Response failures that must be met or exceeded within the
polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.
```

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm
model, the system assumes it is identical to the high threshold.

Usage
Use this command to set an alert or an alarm when the number of A11 Registration Response failures is equal
to or greater than a specified number.
Alerts or alarms are triggered for the number of A11 Registration Response failures based on the following
rules:

- **Enter condition**: Actual number of A11 Registration Response failures > High Threshold
- **Clear condition**: Actual number of A11 Registration Response failures £ Low Threshold

Example
The following command configures a number of A11 Registration Response failures threshold of 1000 and a low
threshold of 500 for a system using the Alarm thresholding model:

```
threshold a11-rrp-failure 1000 clear 500
```
PDSN Service Configuration Mode Commands

threshold a11-rrp-failure
threshold a11-rrq-msg-discard

Set an alarm or alert based on the number of Discarded A11 Registration Requests for the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

threshold a11-rrq-msg-discard high_thresh [ clear low_thresh ]

no threshold a11-rrq-msg-discard

no

Deletes the alert or alarm.

high_thresh
Default: 0
The high threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear low_thresh
Default: 0
The low threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Requests is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of Discarded A11 Registration Requests based on the following rules:

• **Enter condition:** Actual number of Discarded A11 Registration Requests > High Threshold
• **Clear condition:** Actual number of Discarded A11 Registration Requests £ Low Threshold

Example

The following command configures a number of Discarded A11 Registration Requests threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

threshold a11-rrq-msg-discard 1000 clear 500
tft-validation wait-timeout

This command configures the TFT validation wait timeout value for QoS changes. The QoS update timer triggers automatic QoS updates based on dynamic policies.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
tft-validation wait-timeout seconds
```

```
no tft-validation wait-timeout seconds
```

```
no

Removes the wait-timeout timer.
```

Usage
Configures the TFT validation wait time value for A11 RRQ for QoS changes. `seconds` must be an integer from 1 through 65535.

Example
Use the following command to set the TFT validation wait-timeout to 5 seconds:

```
tft-validation wait-timeout 5
```
threshold a11-rac-msg-discard

Set an alarm or alert based on the number of Discarded A11 Registration Acknowledgements for the PDSN service.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold a11-rac-msg-discard high_thresh [ clear low_thresh ]
no threshold a11-rac-msg-discard
```

**no**
Deletes the alert or alarm.

**high_thresh**
Default: 0
The high threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

**clear low_thresh**
Default: 0
The low threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Use this command to set an alert or an alarm when the number of Discarded A11 Registration Acknowledgements is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of Discarded A11 Registration Acknowledgements based on the following rules:

- **Enter condition**: Actual number of Discarded A11 Registration Acknowledgements > High Threshold
- **Clear condition**: Actual number of Discarded A11 Registration Acknowledgements ≤ Low Threshold

**Example**
The following command configures a number of Discarded A11 Registration Acknowledgements threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:
threshold all-rac-msg-discard 1000 clear 500
threshold all-ppp-send-discard

Set an alarm or alert for the PDSN service based on the number of packets that the PPP protocol processing layer internally discarded on transmit for any reason.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

threshold all-ppp-send-discard high_thresh [clear low_thesh]
no threshold all-ppp-send-discard

no
Deletes the alert or alarm.

high_thesh
Default: 0
The high threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear low_thesh
Default: 0
The low threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Use this command to set an alert or an alarm when the number of discarded PPP send packets is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of discarded PPP send packets is based on the following rules:
• Enter condition: Actual number of discarded PPP send packets > High Threshold
• Clear condition: Actual number of discarded PPP send packets £ Low Threshold

Example
The following command configures a number of discarded PPP send packets threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

threshold all-ppp-send-discard 1000 clear 500
PDSN Service Configuration Mode Commands

threshold all-ppp-send-discard
**threshold init-rrq-rcvd-rate**

Set an alarm or alert based on the average number of calls setup per second for the context.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold init-rrq-rcvd-rate
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Deletes the alert or alarm.

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
</tbody>
</table>
| The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 1000000.

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
</tbody>
</table>
| The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second > High Threshold
- **Clear condition:** Actual number of calls setup per second £ Low Threshold

**Example**
The following command configures a number of calls setup per second threshold of **1000** and a low threshold of **500** for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```
Chapter 165
PDSN Service RoHC Configuration Mode Commands

The PDSN Service RoHC Configuration Mode is used to configure RoHC (Robust Header Compression) parameters the PDSN service conveys to the PCF in the initial A11 RRP message before PPP authentication.

Important: The commands, keywords and variables in this mode are available dependent on platform type, product version, and installed license(s).
threshold init-rrq-rcvd-rate
cid-mode

This command enters the RoHC Profile Compression Options Configuration mode. This mode allows you to configure options that apply during RoHC compression for the current RoHC profile.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
cid-mode { large | small } max-cid integer
```

default cid-mode

default
Reset all options in the RoHC Profile Compression Configuration mode to their default values.

large
Use large packets with optional information for RoHC

small
This is the default packet size.
Use small RoHC packets.

max-cid integer
Default: 15
The highest context ID number to be used by the compressor. integer must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.

Usage
Use this command to set the RoHC packet size and define the maximum

Example
The following command sets large RoHC packet size and sets the maximum CID to 100:

```
cid-mode large max-cid 100
```

The following command sets the cid-mode to the default settings of small packets and max-cid 0:

```
default cid-mode
```
end

Returns the CLI prompt to the Exec mode.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits this configuration mode and returns to the PDSN Service configuration mode.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the PDSN Service configuration mode.
mrru

This command sets the size of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments. The size includes the CRC. If MRRU is negotiated to be 0, no segment headers are allowed on the channel.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

mrru num_octets

default mrru

default
reset the value of this command to its default setting

num_octets
Default: 0
This is the number of octets for the maximum size of the largest reconstructed reception unit allowed. num_octets must be an integer from 0 through 65535.

Usage
Use this command to set the size, in octets, of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments.

Example
The following command sets the largest reconstructed reception unit to 1024 octets:

mrru 1024

The following command resets the mrru size to its default of 0 octets:

default mrru
profile

This command specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

profile { [ esp-ip ] [ rtp-udp ] [ udp-ip ] [ uncompressed-ip ] }

default profile

default
Default: esp-ip rtp-udp udp-ip uncompressed-ip
This command sets the RoHC profile configuration back to its default setting.

default

esp-ip
This enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.

rtp-udp
This enables RoHC Profile 0x0001 which is for RTP/UDP/IP compression

udp-ip
This enables RoHC Profile 0x0002 which is for UDP/IP compression, compression of the first 12 octets of the UDP payload is not attempted.

uncompressed-ip
This enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.

Usage

Use this command to specify the RoHC header compression profiles to use.

Example

The following command sets the profiles to use as esp-ip and rtp-udp:

profile esp-ip rtp-udp
Chapter 166
Peer-Server Configuration Mode Commands

The Peer-Server configuration mode provides the commands to define and manage the peer server configuration part of the SS7 routing on an SGSN.

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

Exits the configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the Global configuration mode.
mode

Configures the operational mode of the peer-server.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
mode { loadshare | standby }
```

- **loadshare**
  Sets the peer-server to load share. This is the default.

- **standby**
  Sets the peer-server to be in standby mode.

Usage

Configure the operational mode of the peer-server.

Example

Configure the peer-server for standby mode.

```
mode standby
```
name

Defines the unique identification - the name - of the peer-server in the SS7 routing domain.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
name name
```

*name* must be a string of 1 to 64 alphanumeric characters to define a unique identification for the peer-server within the specific SS7 routing domain. Double quote must be used to create a name that includes spaces.

Usage
Create an easily remembered alphanumeric name for the peer-server.

Example

```
name "Berlin West"
```
pssp

Creates the peer-server-process (PSP) instance and enters the PSP configuration mode. See the PSP Configuration Mode chapter in this guide for information on the configuration commands.

⚠️ **Important:** This command configures a mandatory parameter in the configuration of the peer server.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no] psp instance id

id

id Uniquely identifies the specific peer-server-process configuration. The Id must be an integer from 1 to 4.
```

**Usage**
Use this command to define the peer-server-process (PSP) instance ID number for the SGSN configuration.

**Example**

```
psp instance 3
```
**routing-context**

Defines the ID of the routing context for the peer-server to use.

**Important:** This command configures a mandatory parameter in the configuration of the peer server.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
routing-context id
```

**Example**

```
routing-context 15
```
self-point-code

This command defines the point-code to identify the SGSN as a peer server.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```plaintext
self-point-code point-code
no self-point-code
```

point-code
Point-code is an SS7-type address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Options include:
- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no
Removes the self-point-code configuration for this linkset in the peer server.

**Important:** Removing the self-point-code will result in the termination of all traffic on this link.

Usage
Use this command to define the point-code to identify the SGSN.

Example

```plaintext
self-point-code 6.192.7
```
Chapter 167
P-GW Service Configuration Mode Commands

The P-GW (PDN Gateway) Service Configuration Mode is used to create and manage the relationship between specified services used for either GTP or PMIP network traffic.
associate

Associates the P-GW service with specific pre-configured services and/or policies configured in the same context.

Product
P-GW

Privilege
Administrator

Syntax

associate { egtp-service name [ lma-service name ] | lma-service name [ egtp-service name ] | qci-qos-mapping name }

no associate { egtp-service | lma-service | qci-qos-mapping }

Usage

Use this command to associate the P-GW service with other pre-configured services and/or policies configured in the same context.

Example

The following command associates this service with an eGTP service called egtp1:

associate egtp-service egtp1
authorize-with-hss

Identifies the function to use for subscriber authorization.

Product
P-GW

Privilege
Administrator

Syntax

[ default | no ] authorize-with-hss

[ default | no ]

Resets the command to the default setting of “authorize locally” from an internal APN authorization configuration.

Usage

Use this command to specify that the system will use the S6b interface to acquire subscriber authorization from a 3GPP AAA server and the HSS.
**P-GW Service Configuration Mode Commands**

---

**dns-client context**

Specifies the context to use where the DNS client resides to send DNS queries.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
dns-client context name
[ default | no ] dns-client context
```

**default**

Returns the command to the default setting of targeting the DNS client in the context where the P-GW service resides.

**no**

DNS query is disabled.

**name**

Specifies the name of the context where the DNS client is used for the resolution of PCSCF-FQDN received from S6b interface. *name* must be an existing context and be from 1 to 79 alpha and/or numeric characters.

**Usage**

Use this command to specify the context where the DNS client resides to perform P-CSCF-FQDN resolution from the S6b interface.

**Example**

The following command identifies the *egress1* context as the context where the DNS client resides:

```
dns-client context egress1
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Administrator

Syntax
   end

Usage
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Administrator

**Syntax**
```
exit
```

**Usage**
Return to the previous mode.
fqdn

Configures a Fully Qualified Domain Name for this P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Product
P-GW

Privilege
Administrator

Syntax

fqdn host domain_name realm realm_name

[ default | no ] fqdn

---

**default**

Returns the command to the default setting of “null”.

---

**no**

Remove the configured FQDN from this services configuration.

---

**host domain_name**

Specifies the domain name of the P-GW service. `domain_name` must be from 1 to 255 alpha and/or numeric characters.

---

**realm realm_name**

Specifies the realm name of the P-GW service. `realm_name` must be from 1 to 255 alpha and/or numeric characters.

---

Usage

Use this command to identify the P-GW service using an FQDN required when sending messages over the S6b interface to a 3GPP AAA server.

---

Example

The following command configures the FQDN for this P-GW service as `123abc.com` with a realm name of `all.com`:

```
fqdn host 123abc realm all.com
```
**gx-li context**

Configures the name of the context where lawful intercept packets are delivered to the lawful intercept server.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
gx-li context name
```

```
default gx-li context
```

**default**

Return the command to the default setting of the P-GW context (where this service resides).

```
name
```

Specifies the name of the context where the LI interface is configured for transmitting LI packets to an LI server. *name* must be from 1 to 79 alpha and/or numeric characters.

**Usage**

Use this command to specify the name of the context where the LI source address is configured to send packets to a LI server. By default, the P-GW context will be used.

**Important:** A LI source IP address and interface must be configured in the context specified by this command.

**Example**

The following command identifies the context to use for LI server traffic as *aaa3*:

```
gx-li context aaa3
```
newcall

Configures the P-GW to accept or reject requests for a static IP address if the address is already in use by another session.

Product
P-GW

Privilege
Administrator

Syntax

newcall duplicate-subscriber-requested-address { accept | reject }

no newcall duplicate-subscriber-requested-address

Usage
Use this command to configure the behavior of the P-GW service when receiving requests for static IP address already in use by other sessions.

Important: This command is only applicable to sessions using services supporting duplicate address abort. These services include HA, GGSN, and P-GW.

Example
The following command allows for the acceptance of requests for static IP addresses already in use by other sessions:

    newcall duplicate-subscriber-requested-address accept
plmn id

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming, or belongs to this network.

**Product**
P-GW

**Privilege**
Administrator

**Syntax**

```
plmn id mcc number mnc number [ primary ]
```

- **mcc number mnc number**
  - `mcc number`: Specifies the mobile country code (MCC) portion of the PLMN’s identifier. `number` is the PLMN MCC identifier and must be an integer value between 100 and 999.
  - `mnc number`: Specifies the mobile network code (MNC) portion of the PLMN’s identifier. `number` is the PLMN MNC identifier and can be configured to any 2 or 3 digit integer value between 00 and 999.

- **primary**
  - When multiple PLMN IDs are configured, the `primary` keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute.

**Usage**
The PLMN identifier is used to aid the P-GW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service.

**Example**
The following command configures the PLMN identifier with an MCC of 462 and MNC of 02:

```
plmn id mcc 462 mnc 02
```
session-delete-delay

Configures a delay in terminating a session.

Product
P-GW

Privilege
Administrator

Syntax

```
session-delete-delay timeout [ msec ]
[ default | no ] session-delete-delay timeout
```

- **default**
  Reset the command to the default setting of 10000 msecs.

- **no**
  Disables the feature.

- **timeout msec**
  Default: 10000
  Specifies the time to retain the session before terminating it. \textit{msec} must be an integer from 1000 to 60000.

Usage
Use this command to set a delay to provide session continuity in case of break-before-make scenario.

Example
The following command sets the session delete delay to the default setting of 10,000 msecs:

```
session-delete-delay timeout
```
Chapter 168
Policy Control Configuration Mode Commands

Policy Control Configuration mode is used to configure the Diameter dictionary, origin host, host table entry and host selection algorithm for IMS Authorization service.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

ims-auth-service svc_name

IMS Authorization Configuration Mode

policy-control

Policy Control Configuration Mode
```
apn-name-to-be-included

This command configures the APN name to be included in CCR Gx messages.

Product
GGSN, IPSG, PGW

Privilege
Security Administrator, Administrator

Syntax

apn-name-to-be-included { gn | virtual }

default apn-name-to-be-included

default
Applies the default setting for this command.
Default: gn

gn | virtual
Specifies which APN name must be sent in the Gx messages.
gn: Send the real APN name.
virtual: Send the virtual APN name if present, else send the real APN name.

Usage
Use this command to configure the APN name to be included in the CCR Gx messages to the PCRF—the real APN name or the virtual APN name.

Example
The following command configures sending the real APN name in Gx messages:

apn-name-to-be-included gn
**custom-reauth-trigger**

This command enables custom reauth event triggers.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
custom-reauth-trigger { none | { preservation-changed | reactivation-changed } + }

default custom-reauth-trigger
```

**default**

Configures the default setting for this command.

**none**

Disables all custom event triggers.
This is the default setting.

**preservation-changed**

Enables preservation-changed event trigger.

**Important:** This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

**reactivation-changed**

Enables reactivation-changed event trigger.

**Important:** This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

**Usage**

Use this command to enable/disable custom reauth event triggers.
It is recommended that the preservation-changed and reactivation-changed triggers both be enabled. As, when the bearer goes into preservation mode with the preservation-changed trigger, the reactivation-changed trigger must also be enabled for the bearer to get reactivated subsequently.
If only the preservation-changed trigger is enabled, and the bearer goes into preservation mode, the bearer will never get reactivated. The reactivation triggers will be ignored. If only the reactivation-changed trigger is enabled, reactivation of the already active bearer does not take place, and the reactivation triggers are ignored.
Example
The following command disables all custom event triggers:

```
custom-reauth-trigger none
```
diameter dictionary

Specifies the Diameter Policy Control Application dictionary for the IMS Authorization Service through Gx/Ty interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter dictionary { Standard | dpca-custom1 | dpca-custom10 | dpca-custom11 |
               dpca-custom12 | dpca-custom13 | dpca-custom14 | dpca-custom15 | dpca-custom16 |
               dpca-custom17 | dpca-custom18 | dpca-custom19 | dpca-custom2 | dpca-custom20 |
               dpca-custom3 | dpca-custom4 | dpca-custom5 | dpca-custom6 | dpca-custom7 | dpca-
               custom8 | dpca-custom9 | gxa-3gpp2-standard | gxc-standard | pdsn-ty | r8-gx-
               standard | std-pdsn-ty | ty-plus | ty-standard }

default diameter dictionary

default
Sets the Diameter dictionary to standard for Gx or Ty interface.

dpca-custom1
Custom-defined Diameter dictionary for the Gx interface.

dpca-custom2
Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom3
Custom-defined Diameter dictionary for the Gx interface in conjunction with IP Services Gateway (IPSG).

dpca-custom4
Standard Diameter dictionary for 3GPP Rel. 7 Gx interface.

dpca-custom5
Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom6 ... dpca-custom20
Custom-defined Diameter dictionaries.

gxa-3gpp2-standard
Gxa 3GPP2 standard dictionary.
diameter dictionary

**gxc-standard**
Gxc standard dictionary.

**pdsn-ty**
Custom-defined Diameter dictionary for Ty interface.

**r8-gx-standard**
R8 Gx standard dictionary.

**standard**
Default: Enabled for Gx support in 3GPP networks.
Standard Diameter dictionary for the 3GPP Rel. 6 Gx interface.

**std-pdsn-ty**
Default: Enabled for Ty support in 3GPP2 networks.
Standard Diameter dictionary for Ty interface.

**ty-plus**
Enhanced custom-defined Diameter dictionary for Ty interface.

**ty-standard**
Specifies standard Diameter dictionary for Ty attributes.

---

**Usage**

Use this command to specify the Diameter dictionary for IMS Authorization Service.

---

**Example**
The following command sets the **standard** dictionary for Diameter Policy Control functions in 3GPP network.

```
diameter dictionary standard
```
diameter host-select reselect

This command controls pacing of the reselection or switching of the PCRF after a change occurs in table configuration for an IMS Authorization Service.

Default: Disabled

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter host-select reselect subscriber-limit subs_limit time-interval duration

{ default | no } diameter host-select reselect

default
Applies the default setting for this command.
Sets the PCRF reselection or switching to default state.

no
Removes the configured PCRF reselection method and disables the reselection or switching of PCRF.

subscriber-limit subs_limit
Specifies the limit of subscribers to switch or reselect the PCRF for subscribers not more than subs_limit in time duration of duration second(s).
subs_limit must be an integer from 1 through 1000000.

time-interval duration
Specifies the time duration, in seconds, to reselect PCRF for subscribers not more than subs_limit in time duration of duration second(s).
duration must be an integer from 1 through 3600.

Usage
Use this command to specify the pacing of reselection or switching of the PCRF in an IMS authorization service..
In case IMS authorization session have been opened on certain PCRF on the basis of the current selection table, and the current active table configuration is changed, the IMSA starts selection procedure for the PCRF. Existing sessions on current PCRF from earlier table is required to close and reopened on the selected PCRF from the new table. This reselection periodicity is controlled by this command and it indicates the number of subscriber sessions subs_limit to be reselected or moved in duration seconds.
For example, if this command is configured with 100 subscribers and 2 seconds, then the system reselects the PCRF for no more than 100 subscribers per 2 seconds.
Example
The following command sets the system to reselect the new PCRF for no more than 1000 subscriber in 15 seconds:

```
diameter host-select reselect subscriber-limit 1000 time-interval 15
```
diameter host-select row-precedence

This command adds/appends rows with precedence to a Diameter host table or MSISDN prefix range table.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
diameter host-select row-precedence precedence_value table { { 1 | 2 } host host_name [ realm realm_id ] [ secondary host host_name [ realm realm_id ] ] | { prefix-table { 1 | 2 } msisdns-prefix-from msisdns-prefix_from msisdns-prefix-to msisdns_prefix_to host host_name [ realm realm_id ] [ secondary host sec_host_name [ realm sec_realms_id ] algorithm { active-standby | round-robin } ] } } [ -noconfirm ]
```

```
no diameter host-select row-precedence precedence_value table { 1 | 2 } | prefix-table { 1 | 2 }
```

Removes the row with the specified precedence from the specified Diameter host table.

```
diameter host-select row-precedence precedence_value table { 1 | 2 } host host_name [ realm realm_id ] [ secondary host sec_host_name [ realm sec_realms_id ] ]
```

This command adds/appends a row in the specified Diameter host table.
In StarOS 8.0, a maximum of 16 rows can be added to a table. In StarOS 8.1 and later, a maximum of 128 rows can be added per table.

**Important:** In StarOS 8.1 and later, `precedence_value` must be an integer from 1 through 128. In StarOS 8.0 and earlier, `precedence_value` must be an integer from 1 through 100.

- `table { 1 | 2 }`: Specifies the Diameter host table to add/append the primary and secondary Diameter host addresses.
- `host host_name`: Specifies the primary host name. `host_name` must be an alpha and/or numeric string of 1 through 127 characters in length.
- `realm realm_id`: Specifies the primary realm ID. `realm_id` must be an alpha and/or numeric string of 1 through 127 characters in length.
- `secondary host sec_host_name [ realm sec_realms_id ]`: Specifies the secondary host name and realm ID:
  - `host sec_host_name`: Specifies the secondary host name. `host_name` must be an alpha and/or numeric string of 1 through 127 characters in length.
  - `realm sec_realms_id`: Specifies the secondary realm ID. `realm_name` must be an alpha and/or numeric string of 1 through 127 characters in length.
no diameter host-select row-precedence precedence_value table prefix-table { 1 | 2 } }

Removes the row with the specified precedence from the specified MSISDN prefix range table.

diameter host-select row-precedence precedence_value table prefix-table { 1 | 2 } msisdn-prefix-from msisdn_prefix_from msisdn-prefix-to msisdn_prefix_to host host_name [ realm realm_id ] [ secondary host sec_host_name [ realm sec Realm_id ] algorithm { active-standby | round-robin } [ -noconfirm ]

Use this command to configure the MSISDN prefix range based PCRF selection mechanism for Rel. 7 Gx interface support, wherein the PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation. This command adds a row in the specified MSISDN prefix range table. A maximum of 128 rows can be added per prefix range table.

row-precedence precedence_value: Specifies precedence of the row in the table.

**Important:** In StarOS 8.1 and later, precedence_value must be an integer from 1 through 128. In StarOS 8.0 and earlier, precedence_value must be an integer from 1 through 100.

prefix-table { 1 | 2 }: Specifies the MSISDN prefix range table to add the primary and/or secondary Diameter host addresses.

msisdn-prefix-from msisdn_prefix_from: For a range of MSISDNs, specifies the starting MSISDN.

msisdn-prefix-to msisdn_prefix_to: For a range of MSISDNs, specifies the ending MSISDN.

**Important:** To enable the Gx interface to connect to a specific PCRF for a range of MSISDNs/subscribers configure msisdn_prefix_from and msisdn_prefix_to with the starting and ending MSISDNs respectively. The MSISDN ranges must not overlap between rows. To enable the Gx interface to connect to a specific PCRF for a specific MSISDN/subscriber, configure both msisdn_prefix_from and msisdn_prefix_to with the same MSISDN.

host host_name: Specifies the primary host name. host_name must be an alpha and/or numeric string of 1 through 127 characters in length.

realm realm_id: Specifies the primary realm ID. realm_id must be an alpha and/or numeric string of 1 through 127 characters in length.

secondary host sec_host_name [ realm sec Realm_id ]: Specifies the secondary host name and realm ID: host sec_host_name: Specifies the secondary host name. sec_host_name must be an alpha and/or numeric string of 1 through 127 characters in length.

algorithm { active-standby | round-robin }: Specifies the algorithm for selection between primary and secondary servers in the MSISDN prefix range table. Default: active-standby

active-standby: Specifies selection of servers in the Active-Standby fashion.

round-robin: Specifies selection of servers in the Round-Robin fashion.

**Important:** The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
-noconfirm
Specifies that the command is to execute without any additional prompt and confirmation from the user.

Usage
Use this command to add, update, or delete rows specified with a precedence from a Diameter host table or MSISDN prefix range table.
In the Rel. 7 Gx implementation, when the Gateway interworks with multiple PCRFs, the Gateway can configure the primary and secondary server based on the MSISDN-prefix range in the MSISDN prefix range table. Using this command, you can add a new prefix row into the MSISDN prefix table.
If a row with the precedence that you add already exists in a table, the existing prefix row is removed and the new row is inserted with the same precedence.

Example
The following command adds a row with precedence 12 in table 2 with primary host name as star_ims1 and secondary host name as star_ims2 to Diameter host table.

diameter host-select row-precedence 12 table 2 host star_ims1 secondary host star_ims2
diameter host-select table

This command selects the Diameter host table or the MSISDN prefix range table, and the algorithm to select rows from the Diameter host table.

Product
All

Privilege
Security Administrator, Administrator

Syntax

diameter host-select table { { 1 | 2 } algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin } | prefix-table { 1 | 2 } } { default | no } diameter host-select table

default
Applies the default setting for this command.

no
Removes previous configuration.
When no table is selected, the system will not communicate with any PCRF for new sessions.

diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin } table { 1 | 2 }

algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin }

Default: round-robin

• ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ]: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.

• prefer-ipv4: Specifies that IPv4 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.

• prefer-ipv6: Specifies that IPv6 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.

• msisdn-modulus: This algorithm divides the MSISDN value in binary without the leading “+” of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.

• round-robin: This algorithm rotates all rows in the active table for selection of the row in round-robin fashion. If no algorithm is specified this is the default behavior.

Important: The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.
**diameter host-select table prefix-table { 1 | 2 }**

Specifies the MSISDN Prefix Range table to be used in case of MSISDN prefix range based PCRF discovery mechanism.

**Usage**

Use this command to configure the Diameter host table and row selection methods to select host name or realm for PCRF.

When this command is used to change which table the system should be using, user must re-determine which E-PDF the system should be using for each subscriber. If a different E-PDF results from the configuration change in the table, the system will wait for all of the IMS sessions for the subscriber to be no longer active and then the system either closes/opens Gx sessions with the old/new PDFs respectively, or the system deactivates the PDP contexts of the subscriber.

Here is an example of how row selection is configured for three hosts that the system will use for load-balancing. Operator can configure six rows in a table, as follows.

<table>
<thead>
<tr>
<th>Modulo 6</th>
<th>Primary Host</th>
<th>Secondary Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

In the above table, the three hosts are named 1, 2, and 3. When all hosts are working, the load will be distributed among all the three hosts. If host 1 fails, then the load will be distributed between the remaining two hosts. In this scenario, the modulo 6 results of 2 and 4 will return rows that have primary hosts but no working back-up host.

In the Rel. 7 Gx implementation, the GGSN/PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation. The ip-address-modulus, msisdn-modulus, and round-robin algorithms are supported by the GGSN/PCEF for PCRF discovery. In addition, the active/standby and round-robin algorithms are used for selection between primary and secondary servers based on the MSISDN Prefix Range Table.

**Example**

The following command specifies `table 1` with `round-robin` algorithm to select the rows with host name for E-PDF in Diameter host table.

```
diameter host-select table 1 algorithm round-robin
```
diameter origin endpoint

This command binds the origin endpoint configured in Context Configuration mode to the IMS Authorization service for Diameter Policy Control Application (DPCA).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
diameter origin endpoint  endpoint_name
```

```
no diameter origin
```

**Usage**

Use this command to bind a configured Diameter origin endpoint to the IMS Authorization service for DPCA. This IMS authorization service searches all system contexts until it finds one with a matching Diameter origin endpoint name specified.

**Example**
The following command binds a configured endpoint named test to the IMS authorization service:

```
diameter origin endpoint test
```
**diameter request-timeout**

This command configures the request-timeout setting for Diameter-IMSA Gx interface.

**Product**  
GGSN

**Privilege**  
Security Administrator, Administrator

**Syntax**

```plaintext
diameter request-timeout timeout
default diameter request-timeout
```

- `default`  
  Applies the default setting for this command.

- `timeout`  
  Specifies the timeout period in seconds.  
  `timeout` must be an integer from 1 through 300.  
  Default: 10 seconds

**Usage**

Use this command to configure the request-timeout setting for Diameter-IMSA Gx interface.

**Example**

The following command configures the Diameter request-timeout setting to 20 seconds:

```plaintext
diameter request-timeout 20
```
end

Exits the current mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to change to the Exec mode.
exit

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
li-secret

This command configures an Lawful Intercept shared secret key value for LI session. This value needs to be the same between PCRF and PCEF for Lawful Interception to happen.

**Product**
MME, P-GW, S-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] li-secret [ encrypted ] key key_value
[ no ] li-secret
```

- **no**
  This keywords removes the configured secret key value for LI. This is the default mode.

- **encrypted**
  This keyword displays the secret value in an encrypted format and only `show configuration` `showsecrets` will make the secret value visible.

- **key key_value**
  This keyword configures a secret key value for Lawful Intercept shared secret key. `key_value` must be an alphabetic and/or numeric string of size 1 to 128 characters.

**Usage**

Use this command to configure a shared secret key value with or without encryption. This value needs to be the same between PCRF and PCEF (network function service node) for Lawful Interception to happen. It this command is not configured, by default LI secret key will be used. The command will display the secret value in an encrypted format and only `show configuration` `showsecrets` command will make the secret value visible.

**Example**

Following command sets the encrypted LI secret key to a value for LI session.

```
li-secret encrypted key secret_key_value
```
failure-handling

This command configures Diameter failure handling behavior.

Product
All

Privilege
Security Administrator, Administrator

Syntax

In StarOS 8.0:

```
failure-handling { continue | retry-and-terminate | terminate | diameter-result-code { any-error | result_code } ccfh { continue | retry-and-terminate | terminate } [ cc-request-type { initial-request | terminate-request | update-request } ] } }

no failure-handling diameter-result-code { any-error | integer result_code } [ cc-request-type { initial-request | terminate-request | update-request } ] }
```

In StarOS 8.1 and later:

```
failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } { diameter-result-code { any-error | result_code [ to end_result_code ] } } { continue | retry-and-terminate | terminate }

no failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } [ diameter-result-code { any-error | result_code{ to end_result_code} ] ] }
```

---

**no**
Disables previous failure-handling configuration.

**continue**
Specifies that in the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.

**retry-and-terminate**
Specifies that in the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

**terminate**
Specifies that in the event of a failure the user session be terminated.

**diameter-result-code { any-error | result_code [ to end_result_code ] }**
Specifies failure handling behavior for any/specific result-code(s) to identify the type of failure and failure handling action for specific credit control request type.
**any-error**: Specifies failure handling behavior for those result-codes for which failure-handling behavior has not been specified.

**result_code**: Specifies a Diameter failure result code. *result_code* is the code returned for a failure handling action and must be an integer from 3000 through 4999.

**to end_result_code**: Use to specify a range of Diameter failure result codes. *end_result_code* must be an integer from 3000 through 4999, and must be greater than *result_code*.

<table>
<thead>
<tr>
<th>continue</th>
<th>retry-and-terminate</th>
<th>terminate</th>
</tr>
</thead>
</table>

As in StarOS 8.1 and later.

Specifies the credit control failure handling action.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.

- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

- **terminate**: In the event of a failure the user session is terminated.

**ccfh { continue | retry-and-terminate | terminate }**

As in StarOS 8.0:

Specifies the credit control failure handling (CCFH) action with or without credit control request type.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.

- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

- **terminate**: In the event of a failure the user session is terminated.

**cc-request-type**

As in StarOS 8.0:

This optional keyword defines the type of credit control request with failure result code and credit control failure handling action for a session.

- **any-request**: Specifies the request type as any request for a new session.

- **initial-request**: Specifies the request type as initial request for a new session.

- **terminate-request**: Specifies the request type as terminate request for a session.

- **update-request**: Specifies the request type as update request for an active session.

**Usage**

Use this command to configure the Diameter Policy Control Application (DPCA) failure handling behavior. When an unknown rulebase comes in CCA, changing of rulebase and failure handling is managed in the following manner:

- If the new and existing rulebases have the same CCA policy, then switch to the new rulebase is successful.

- If the new rulebase is valid and has CCA-enabled, in CCA-Initial/Update request, switch to the new rulebase is successful.
• If the new rulebase is valid and does NOT have CCA enabled, whereas the existing rulebase has credit enabled, or vice versa, in CCA-Initial/Update request:

  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY&TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.

• If the new rulebase is invalid, in CCA-Initial/Update request:

  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY&TERMINATE: Terminates on successful CCA-T, or terminates after successful/failed retry to secondary.
  - CCFH-TERMINATE: Terminates on successful/failed CCR-T to Primary.

The default failure handling behavior is:

```
failure-handling diameter-result-code any-error ccfh terminate
```

---

**Example**

The following command sets the DPCA failure handling to `retry-and-terminate` and return a result code of 3456 for credit control request type `initial-request`:

As in StarOS 8.0:

```
failure-handling diameter-result-code 3456 ccfh retry-and-terminate cc-request-type initial-request
```

As in StarOS 8.1 and later:

```
failure-handling cc-request-type initial-request diameter-result-code 3456 retry-and-terminate
```
reauth-trigger

This command specifies the trigger events to initiate re-authorization for a subscriber in IMS authorization service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ default ] reauth-trigger { all | { an-gw-change | bearer-loss | bearer-recovery | plmn-change | policy-failure | qos-change | rat-change | sgsn-change | tft-change | tft-delete } + }
```

**Default**
Applies the default setting for this command.

**all**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on all events listed in this command.

**an-gw-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber whose access network gateway changed.

**bearer-loss**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on loss of bearer or service.

**bearer-recovery**
Sets the IMS authorization service to initiate re-authorization process for a subscriber when a bearer or service recovered after loss of bearer or service.

**default-bearer-qos-change**
Sets the IMS authorization service to initiate re-authorization process when QoS is changed and DEFAULT_EPS_BEARER_QOS_CHANGE event triggered for the default EPS bearer context of a subscriber in LTE network.

**plmn-change**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Public Land Mobile Network (PLMN) of subscriber.

**policy-failure**
Sets the IMS authorization service to initiate re-authorization process for a subscriber on failure of credit and charging policy for subscriber.
\textbf{qos-change}
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Quality of Service level/rating of subscriber.

\textbf{rat-change}
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Radio Access Type (RAT) of subscriber node.

\textbf{sgsn-change}
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in SGSN for subscriber node.

\textbf{tft-change}
Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Traffic Flow Template (TFT) of subscriber session.

\textbf{tft-delete}
Sets the IMS authorization service to initiate re-authorization process for a subscriber when Traffic Flow Template (TFT) of subscriber session is deleted by a system administrative user.

\textbf{Usage}
Use this command to set the triggers to initiate QoS re-authorization process for a subscriber in IMS authorization service.

\textbf{Example}
Following command sets the re-authorization trigger to \texttt{bearer-loss}, so that re-authorization of subscriber session is initiated on loss of bearer.

\texttt{reauth-trigger bearer-loss}
Chapter 169
PVC Configuration Mode Commands

The Permanent Virtual Connection (PVC) configuration mode commands bind IP interfaces or SS7-Frame Relay links a PVC as well as configure PVC operational parameters for a specific port.

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

This command binds IP interface or SS7 link to the PVC.

**Important:** Prior to attempting the binding, the interface and context or the SS7 routing information and link must have been configured.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bind { interface interface_name context_name | link ss7-routing-domain rd_id linkset-id id link-id id}  
no bind { interface interface_name | link ss7-routing-domain rd_id linkset-id id link-id id}  
no
```

- **interface_name**
  Defines the name of the virtual interface to be bound to the PVC. `interface_name` must be a unique string consisting of 1 to 79 alphanumeric characters.

- **context_name**
  Specifies the name of the context to be bound to the virtual interface. `context_name` must be a unique string consisting of 1 to 79 alphanumeric characters.

- **ss7-routing-domain rd_id**
  Identifies a specific SS7 routing domain. `rd_id` must be an integer from 1 to 12

- **linkset-id id**
  Identifies a specific linkset within the routing domain. `id` must be an integer from 1 to 33

- **link-id id**
  Identifies a specific link within the linkset. `id` must be an integer value 1 - 16

**Usage**

Use this command to bind the PVC to an interface or a specific link.
PVC Configuration Mode Commands

Example

bind ss7-routing-domain 1linkset-id 23link-id 2
**encapsulation aal5**

Specify the data encapsulation type for the ATM adaptation layer 5 (AAL5) frames for the PVC.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
encapsulation aal5 { llc-snap | vc-mux }
```

- **llc-snap**
  Frames protocol is identified in the AAL5 using logical link control (LLC) encapsulation.

- **vc-mux**
  Frames are not encapsulated and use virtual circuit multiplexing (VC-MUX) to identify the protocols used for the AAL5 frames.

**Usage**
Use this command to identify the protocol type for the circuit.

**Example**

```
encapsulation aal5 vc-mux
```
end

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

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the PVC configuration mode and returns to the ATM port configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**

Return to the port configuration mode.
shaping

Specify the type of traffic shaping (rates) for this PVC.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
shaping { cbr pcr pcr_num | ubr pcr pcr_num | ubr+ pcr pcr_num mrc mrc_num | vbr pcr pcr_num scr src_num mbs mbs_num }
```

- **cbr**
  Constant bit rate
  - pcr - peak cell rate = cells per second
  - `pcr_num` must be an integer from 75 to 1412830

- **ubr**
  Unspecified Bit Rate
  - pcr - peak cell rate = cells per second
  - `pcr_num` must be an integer from 75 to 1412830

- **ubr+**
  Unspecified Bit Rate with Minimum Cell Rate.
  The PCR and MCR values should be set to maintain the following relationship: \( PCR \geq (MCR + \text{minRate}) \),
  where the current recommended minRate is 75.
  - pcr - peak cell rate = cells per second
  - `pcr_num` must be an integer from 75 to 1412830
  - mcr - minimum cell rate
  - `mrc_num` must be an integer from 75 to 1412830

- **vbr**
  Variable Bit Rate, NRT (not real time) type.
  The PCR and MCR values should be set to maintain the following relationship: \( PCR \geq (MCR + \text{minRate}) \),
  where the current recommended minRate is 75.
  - pcr - peak cell rate = cells per second
  - `pcr_num` must be an integer from 75 to 1412830
  - scr - sustained cell rate
  - `src_num` must be an integer from 75 to 1412830
  - mbs - maximum burst size
  - `mbs_num` must be an integer from 75 to 1412830

Usage

Use this command to configure the shaping for egress traffic on this PVC.
Example

shaping cbr pcr 56000
**shutdown**

Disables/enables traffic over the current VLAN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
shutdown
no shutdown
```

**Usage**

Enables the VLAN. When omitted the VLAN is shutdown.

```
no
```

Enables/Disables specified port or card. Command action depends on mode issued from. Shut down a VLAN. This command is necessary to bring a VLAN into service by enabling it via the `no` keyword.

**Example**

To disable a VLAN from sending or receiving network traffic use the following command:

```
shutdown
```

To enable a VLAN use the following command:

```
no shutdown
```
Chapter 170
PVC Interface Configuration Mode Commands

The PVC (permanent virtual connection) Interface configuration mode is used to create and manage the IP parameters for PVC interface(s) associated with an OLC (ATM-type) for a specific context.

All configuration information specified with these commands is displayed using the Exec mode.

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

Defines descriptive text to provide useful information about the current interface.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

description text

no description

**no**
Erases the port’s description from the configuration file.

text

text: must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

**Usage**
Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters, 79.

**Example**

description "PVC12 connects server 1 to home office."
**end**

Exits the PVC interface configuration mode and returns to the Exec mode.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the interface configuration mode and returns to the context configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the context configuration mode.
The commands in this section are used to configure the IP parameters for the PVC interface.

**Important:** Before configuring the OSPF parameters in this section, you need to enable OSPF using the router command and OSPF configuration sub-mode commands accessed in the Context configuration mode and documented in the Context Configuration Mode chapter of this Command Line Interface Reference.
**ip access-group**

This command identifies the access control list (ACL) to be associated with this PVC interface in this context.

**Important:** Prior to using this command, the access list must be created for this context with the `ip access-list` command in the Context configuration mode and then the ACL must be configured using the commands described in CLI chapter ACL Configuration Mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip access-group name { in | out }
no ip access-group name { in | out }
```

- `no`
  Indicates the specified access group to be removed from the access list.

- `name`
  Specifies the access control list (ACL) rule to be added or removed from the group.
  `name` is a string of 1 to 79 alpha and/or numeric characters with no spaces.

**Important:** Up to 8 ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128 rule limit for the interface.

```
in | out
in: specifies list is for in-bound access control.
out: specifies the list is for out-bound access control.
```

**Important:** Even though “in” or “out” can be specified, context-level ACL rules are automatically applied to both directions.

**Usage**

Use this command to add IP access lists configured for the same context to an IP access-group. The list can be configured to apply to all inbound and/or outbound traffic.

**Example**
The following adds ACL access-list-1 to the IP access-group associated with this PVC for this context.

```
ip access-group access-list-1 in
```
### ip address

Defines the primary IP address and the network mask to be associated with this PVC interface for this context. This command can also be used to configure the secondary IP address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip address ip_address ip_mask [ secondary ]

no ipaddress ip_address
```

**Usage**

Configures or deletes the IPv4 or IPv6 addresses and subnet mask to be associated with this PVC.

**Example**

The following configures the secondary IP address to associate with the interface.

```
ip address 131.2.3.4 255.255.255.0 secondary
```

The following set of commands removes the primary IP address from the PVC interface configuration for this context.

```
no ip address secondary address
no ip address primary address
```
**ip mtu**

Configures the maximum transmission unit (MTU) to be supported on this interface.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip mtu value
no ip mtu
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables and/or restores the option to the system default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>mtu value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the maximum transmission unit in octets.</td>
</tr>
<tr>
<td><em>value</em>: Enter an integer between 576 and 1600. Default is 1500.</td>
</tr>
</tbody>
</table>

**Usage**

Change the maximum transmission unit size to 1300.

**Example**

```
ip mtu 1300
```
**ip ospf authentication-key**

This command configures the password or key to be used for OSPF (Open Shortest Path First) authentication with neighboring routers.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

- **no**
  Deletes the authentication key.

- **encrypted**
  Enter this keyword if you are pasting a previously encrypted authentication key into the `password auth_key` for this command.

- **password auth_key**
  `auth_key` is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication key (password). This variable is entered in clear text format.

**Usage**
Use this command to set the authentication key used when authenticating with neighboring routers.

**Example**
To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```
ip ospf authentication-type

This command configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
ip ospf authentication-type { message-digest | null | text }
no ip ospf authentication-type { message-digest | null | text }
```

- **no**
  Disable this function.

- **message-digest**
  Set the OSPF authentication type to use the message digest (MD) authentication method.

- **null**
  Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

- **text**
  Set the OSPF authentication type to use the clear text authentication method.

Usage

Use this command to set the type of authentication to use when authenticating with neighboring routers.

Example

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```
**ip ospf cost**

This command configures the cost associated with sending a packet over this logical interface.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip ospf cost value

no ip ospf cost
```

---

**no**
Disable this function.

**value**
Default: 10
The cost to assign to OSPF packets. This must be an integer from 1 through 65535.

---

**Usage**
Use this command to set the cost associated with routes from the interface.

---

**Example**
Use the following command to set the cost to 20;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```
ip ospf dead-interval

This command configures the dead-interval and the delay time in seconds, for OSPF communications.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
ip ospf dead-interval value
no ip ospf dead-interval
```

no
- Deletes the value set and returns the value to its default.

value
- The interval, in seconds, that the router should wait. During this interval, if no packets are received then the system considers the neighboring router to be off-line. This interval is typically 4 times the duration of the hello-interval.
- value must be an integer from 1 through 65535. Default: 40

Usage
Use this command to set the dead-intervals or delays for OSPF communications.

Example
To set the dead-interval to 100, use the following command:

```
   ip ospf dead-interval 100
```

To delete the setting for the dead-interval and reset the dead-interval value to its default of 40, use the following command:

```
   no ip ospf dead-interval
```
ip ospf hello-interval

This command configures the delay time in seconds, for OSPF hello interval.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip ospf hello-interval value
no ip ospf hello-interval
```

- **no**
  Deletes the value set and returns the value to its default.

- **value**
  The interval, in seconds, between sending hello packets. This value is typically set to be 1/4 of the value of the **dead-interval**.
  value must be an integer from 1 through 65535. Default: 10

**Usage**
Use this command to set the delays for the hello-interval.

**Example**
To set the hello-interval to 25, use the following command;

```
ip ospf hello-interval 25
```

To delete the setting for the hello-interval and reset the hello-interval value to its default of 10, use the following command

```
no ip ospf hello-interval
```
ip ospf message-digest-key

This command enables the use of MD5-based OSPF authentication.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
ip ospf message-digest-key key_id md5 [ encrypted ] password authentication_key
no ip ospf message-digest-key key_id
```

no
Deletes the key.

```
message-digest-key key_id
```
Specifies the key identifier number. key_id must be an integer from 1 through 255.

```
encrypted
```
Use this if you are pasting a previously encrypted authentication key into the CLI command.

```
password authentication_key
```
The password to use for authentication. authentication_key is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication password. This variable is entered in clear text format.

Usage
Use this command to create an authentication key that uses MD5-based OSPF authentication.

Example
To create a key with the ID of 25 and a password of 123abc, use the following command;

```
   ip ospf message-digest-key 25 md5 password 123abc
```
To delete the same key, enter the following command;

```
   no ip ospf message-digest-key 25
```
**ip ospf network**

Configures the OSPF network type.

**Product**
- SGSN

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ip ospf network
```

- **no**
  Disable this function.

- **broadcast**
  Sets the network type to broadcast.

- **non-broadcast**
  Sets the network type to non-broadcast multi access (NBMA).

- **point-to-multipoint**
  Sets the network type to point-to-multipoint.

- **point-to-point**
  Sets the network type to point-to-point.

**Usage**

Use this command to specify the OSPF network type.

**Example**

To set the OSPF network type to broadcast, enter the following command:

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command:

```
no ip ospf network
```
**ip ospf priority**

This command designates the OSPF router priority.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ip ospf priority value
no ip ospf priority value
```

**Usage**

Use this command to set the OSPF router priority.

**Example**

To set the priority to 25, enter the following command:

```
ip ospf priority 25
```

To disable the priority, enter the following command:

```
no ip ospf priority
```
**ip ospf retransmit-interval**

This command configures the retransmit-interval and the delay time in seconds, for OSPF communications.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip ospf dead-interval value
no ip ospf dead-interval
```

**Usage**
Use this command to set the retransmit-intervals or delays for OSPF communications.

**Example**
To set the dead-interval to 25, use the following command;

```
ip ospf retransmit-interval 25
```
ip ospf transmit-delay

This command configures the transmit-delay the OSPF communications parameters.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
ip ospf transmit-delay value
no ip ospf transmit-delay
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Deletes the value set and returns the value to its default.</td>
</tr>
<tr>
<td>transmit-delay value</td>
<td>The interval, in seconds, that the router should wait before transmitting a packet. value must be an integer from 1 through 65535. Default: 1</td>
</tr>
</tbody>
</table>

Usage
Use this command to set the transmit-delay.

Example
To set the transmit delay to 5 seconds, use the following command;

```
ip ospf transmit-delay 5
```

To delete the setting for the transmit-delay or reset the transmit-delay value to its default of 1, use the following command

```
no ip ospf transmit-delay
```
Chapter 171
QCI - QoS Mapping Configuration Mode Commands

The QoS Class Index (QCI) to QoS Mapping Configuration Mode is used to map QoS Class Indexes to enforceable QoS parameters. Mapping can occur between the RAN and the Serving Gateway (S-GW), the Mobility Management Entity (MME), and/or the PDN Gateway (P-GW) in an LTE network or between the RAN and the eHRPD Serving Gateway (HSGW) in an eHRPD network.

```
Exec Mode

configure

Global Configuration Mode

qci-qos-mapping name

QCI – QoS Mapping Config Mode
```
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage

Return to the previous mode.
qci

Creates and maps QCI values to enforceable QoS parameters.

Product
HSGW, P-GW, S-GW

Privilege
Administrator

Syntax

qci num

[ delay-class num precedence-class num reliability-class num

[ downlink { encaps-header { copy-inner | dscp-marking hex } | user-datagram
dscp-marking hex [ encaps-header { copy-inner | dscp-marking hex } ] } ]

[ gbr ]

[ max-packet-delay num max-error-rate num

[ non-gbr ]

[ uplink { encaps-header { copy-inner | dscp-marking hex } | user-datagram dscp-
marking hex [ encaps-header { copy-inner | dscp-marking hex } ] } ]

[ default | no ] qci num

  default
  Resets the default values for the select QCI value.

  no
  Disables the selected QCI value.

  num
  Specifies the QCI value to be enabled. num must be an integer value between 1 and 32.
  QCI values 1 through 9 are standard values. Only undefined values (10 through 32) can be defined.

Important: QCI values 1 through 9 are defined in the 3GPP Specification TS 23.203 “Policy and charging control architecture”.

delay-class num precedence-class num reliability-class num

delay-class num: Pre-release 8 value for configuring packet delay. num must be an integer value between 1 and 32.
precedence-class num: Pre-release 8 value for configuring packet precedence. num must be an integer value between 1 and 32.
reliability-class num: Pre-release 8 value for configuring packet reliability. num must be an integer value between 1 and 32.

downlink { encaps-header { copy-inner | dscp-marking hex } | user-datatype dscp-marking hex [ encaps-header { copy-inner | dscp-marking hex } ] } }

Configures parameters for downlink traffic.
encaps-header: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
user-datatype dscp-marking hex: Specifies that the UDP DSCP marking is to be defined by this keyword. hex must be an integer value between 1 and 32.

{ copy-inner | dscp-marking hex }

•copy-inner: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.

•dscp-marking hex: Specifies that the DSCP marking is to be defined by this keyword. hex must be an integer value between 1 and 32.

gbr

Specifies that this QCI type is Guaranteed Bit Rate (GBR).

max-packet-delay num max-error-rate num

max-packet-delay num: Specifies the maximum packet delay in milliseconds that can be applied to the data with the QCI. num must be an integer value from 1 through 1000. Default is 10ms for QCI values greater than 9.
max-error-rate num: Specifies the maximum error loss rate of non-congestion related packet loss. num must be an integer value from 1 through 6 specifying 10-1 through 10-6. Default is 3 (or 10-3) for QCI values greater than 9.

Important: Defaults for QCI values less than 9 are defined in the 3GPP Specification TS 23.203 “Policy and charging control architecture”.

non-gbr

Specifies that this QCI type is non-Guaranteed Bit Rate (non-GBR).

uplink { encaps-header { copy-inner | dscp-marking hex } | user-datatype dscp-marking hex [ encaps-header { copy-inner | dscp-marking hex } ] } }

Configures parameters for uplink traffic.
encaps-header: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
user-datatype dscp-marking hex: Specifies that the UDP DSCP marking is to be defined by this keyword. hex must be an integer value between 1 and 32.

{ copy-inner | dscp-marking hex }

•copy-inner: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.

•dscp-marking hex: Specifies that the DSCP marking is to be defined by this keyword. hex must be an integer value between 1 and 32.
Use this command to create and map QCI values to enforceable QoS parameters.

**Example**
The following command creates a QCI value of 15 and defines the uplink encapsulation header as using the DSCP marking from the encapsulated UDP header:

```
qci 15 uplink encaps-header copy-inner
```
Chapter 172
QCI - RAN ID Mapping Configuration Mode Commands

The QoS Class Index (QCI) Mapping Configuration Mode is used to map RAN profile IDs to QoS Class Indexes via the HRPD Serving Gateway (HSGW) in an eHRPD network.

- Exec Mode
- configure
- Global Configuration Mode
- profile-id-qci-mapping-table name
- QCI – RAN ID Mapping Config Mode
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
   exit

Usage
Return to the previous mode.
profile-id

Maps a QCI ID to a RAN profile ID and modifies data flow bit rate ranges.

Product
HSGW

Privilege
Administrator

Syntax

```
profile-id  id  qci  num  [  uplink  {  gbr  rate  [  mbr  rate  ]  |  mbr  rate  [  gbr  rate  ]  }  
            downlink  {  gbr  rate  [  mbr  rate  ]  |  mbr  rate  [  gbr  rate  ]  }  ]
```

```
o  profile-id  id
```

- **no**
  Removes the specified profile ID entry from this map.

- **id**
  Specifies the profile ID to which a QCI ID will be mapped. `id` must be an integer value from 1 to 65535.

- **qci  num**
  Specifies the QCI number to which the profile ID will be mapped. `num` must be an integer value from 1 to 255.

- **uplink**
  Specifies that the guaranteed bit rate (GBR) and/or maximum bit rate (MBR) setting that follow this keyword will be applied to the uplink data flow.

- **downlink**
  Specifies that the guaranteed bit rate (GBR) and/or maximum bit rate (MBR) settings that follow this keyword will be applied to the downlink data flow.

- **gbr  rate**
  Specifies the guaranteed bit rate for the uplink or downlink data flow. `rate` must be an integer value from 0 to 4294967295.

- **mbr  rate**
  Specifies the maximum bit rate for the uplink or downlink data flow. `rate` must be an integer value from 0 to 4294967295.

Usage

Use this command to map a QCI ID to a RAN profile ID and, optionally, modify data flow bit rate ranges.
Example
The following command maps a QCI ID (1) to a profile ID (10) and sets the uplink guaranteed bit rate to 10000 and the downlink guaranteed bit rate to 20000:

```
profile-id 10 qci 1 uplink gbr 10000 downlink gbr 20000
```
Chapter 173
Radio Network Controller (RNC) Configuration Mode Commands

The Radio Network Controller (for release 8.0) or RNC (for releases 8.1 and higher) configuration mode defines the parameters related to the SGSN connection with an RNC.

The command prompt for this mode will appear as:

```
<context_name> <hostname>(config-ctx-iups-service-rnc)#
```

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate-gtpu-bind-address

This command defines the GTP-U loopback address and associates (binds) this address with a particular interface (non-loopback) address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] associate-gtpu-bind-address ip_address to-interface-address ip_address
```

- **no**
  - Removes the loopback address definition and interface association from the current RNC configuration.

- **ip_address**
  - Must be specified using the standard IPv4 dotted decimal notation.

**Usage**

Use this command to setup an association between a loopback address and a non-loopback address.

**Example**

```
associate-gtpu-bind-address x.x.x.x to-interface-address y.y.y.y
```
description

This command defines an alphanumeric string that is intended to provide descriptive information about the radio network controller (RNC). This is used for operator reference only.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

description string

no description

Syntax:

no
- Removes the description string from the current RNC configuration.

string
- Specifies the alphanumeric string that is stored. Must be from 1 through 255 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

Usage
Use this command to set a description for reference by operators.

Example
The following command sets the description to identify an RNC.

description "RNC1 Carrier2 Uganda"
**direct-tunnel**

This command enables/disables the direct tunnel feature through the interface to the radio network controller (RNC).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
direct-tunnel not-permitted-by-rnc
default direct-tunnel
```

- **default**
  Sets the direct tunnel support on RNC to default mode; i.e. enabling direct tunnel.

- **not-permitted-by-rnc**
  Default: enabled
  Disables the direct-tunnel support on radio network controller (RNC).

**Usage**
Use this command to disable/enable the direct-tunnel function on RNC.

**Example**
Following command disables the direct tunnel support on RNC:

```plaintext
direct-tunnel not-permitted-by-rnc
```
end

Exits the configuration mode and returns to the Exec mode.

Product  
All

Privilege  
Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the Global configuration mode.
**lac**

This command identifies a Local Area Concentrator (LAC) and a Remote Area Concentrator (RAC) and associates them with this RNC definition.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

\[
\text{[no]} \text{ lac} \text{ lac_id rac rac_id}
\]

- **no**
  Deletes the LAC and RAC information from the system configuration.

- **lac_id**
  A unique numeric identifier for the LAC associated with the RNC.
  \text{lac_id} must be an integer between 1 and 65535.

- **rac_id**
  A unique numeric identifier for the RLAC associated with the RNC.
  \text{rac_id} must be an integer between 1 and 255.

**Usage**

Creates an association with a specific LAC and RAC.

**Example**

\text{lac 545 rac 23}
overload-action disable

This command maps an action to be taken if traffic reaches or exceeds defined levels. The command can be re-entered multiple times to create definitions for each parameter.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms }

traffic-level traffic-level

[ no | default ] overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms }

no
Removes the defined overload action from configuration.

default
Resets the traffic level to the default level for the associated overload action.

activate traffic-level traffic-level
The system rejects new requests to activate PDP contexts if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 14

attach traffic-level traffic-level
The system rejects new requests for GPRS attach if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 15

auth-challenge traffic-level traffic-level
The system skips performing authentication challenges if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 4

modify-request traffic-level
The system rejects requests to modify a PDP context if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 12
Radio Network Controller (RNC) Configuration Mode Commands

overload-action disable

---

**paging-downlink-data traffic-level traffic-level**

If the defined traffic-level is exceeded, then paging is not performed for data during downlinks if RABs are not available.

traffic-level: An integer 1 to 15.

Default: 11

---

**ptmsi-reallocation traffic-level traffic-level**

The system skips performing ptmsi-reallocation if the defined traffic-level is reached or exceeded.

traffic-level: An integer from 1 to 15.

Default: 4

---

**service-request-data traffic-level traffic-level**

The system rejects service requests to accept data and establish new RABs if the defined traffic-level is reached or exceeded.

traffic-level: An integer from 1 to 15.

Default: 10

---

**sms traffic-level traffic-level**

The system rejects SMS signaling if the defined traffic-level is reached or exceeded.

traffic-level: An integer 1 to 15.

Default: 8

---

**Usage**

Instruct the system to reject service requests to establish new RABs if the traffic level reaches 3.

---

**Example**

overload-action disable service-request-data traffic-level 3
paging-non-searching-indication

This command instructs the SGSN to include the non-searching indicator flag in the page-request message.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

paging-non-searching-indication { non-searching | searching }

[ no | default ] paging-non-searching-indication

no | default
This is the default. Entering no or default with this command disables the inclusion of the flag.

non-searching
Set the non-searching-indication to non-searching in the page-request message.

searching
Set the non-searching-indication to searching in the page-request message.

Usage
Use this command to determine which type of search indicator flag will be included in the page-request message.

Example

paging-non-searching-indication non-searching
pointcode

Configures the point code of the RNC.
The access protocol that is part of the IuPS Service configuration mode must be configured prior to defining the RNC’s point code.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] pointcode pt_code

no
Deletes the RNC’s point code information from the system configuration.

pt_code
Point code in dotted-decimal format:
● ITU Range 0.0.1 to 7.255.7
● ANSI Range 0.0.1 to 255.255.255
● TTC Range 0.0.1 to 15.31.255
● string of 1 to 11 characters

Usage
Use this command to identify the point code of the associated RNC.

Example

pointcode 1.234.2
rab-modify-procedure

This command configures how the RAB (radio access bearer) assignment procedure will be modified.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
rab-modify-procedure { normal-modify | release-and-establish }
```

```
default rab-modify-procedure
```

default
Returns the configuration to the default setting for this command parameter.

```
normal-modify
```

Selects the normal RAB modify procedure.

```
release-and-establish
```

Instructs the system to release and establish the RAB procedure.

**Usage**

Set the procedure to establish the radio access bearer (RAB).

**Example**

```
rab-modify-procedure normal-modify
```
ranap paging-cause-ie

This command sets the paging cause value and either includes or suppresses the Paging Cause IE in responses to Paging Requests due to various sources. This command is available in releases 8.1 and higher.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```text

| default | no | ranap { paging-cause-ie { all | background-data | conversational-data | gmm-signalling | gs-signalling | interactive-data | sm-signalling | sms-signalling | streaming-data }

---

default
Resets the specific parameters value to default.

---

no
Suppresses the Paging Cause IE so that it is not included in responses to Paging Requests from respective sources.

---

all
Using all sets the action for the Paging Cause IE value for all paging due to all sources.

---

background-data [ value ]
Default: 3 (terminating background call)
Set the Paging Cause IE value for paging due to background data.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

---

conversational-data [ value ]
Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to conversational data.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

---

gmm-signalling [ value ]
Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to gmm-signalling.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.
**gs-signalling** [ value ]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to VLR Paging Request.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**interactive-data** [ value ]

Default: 2 (terminating interactive call)
Set the Paging Cause IE value for paging due to interactive data.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**sm-signalling** [ value ]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to SM signaling.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**sms-signalling** [ value ]

Default: 4 (terminating low priority signaling)
Set the Paging Cause IE value for paging due to SMS signaling.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**streaming-data** [ value ]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to streaming data.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**Usage**

This command can be used to set the value (meaning) of the Paging Cause IE included in responses to Paging Requests or it can be used to suppress the inclusion of the Paging Cause IE in the responses. These actions can be configured for paging for all sources or for a specified source.

The following values are applicable to all Paging Cause IEs:
- 0 - Terminating conversational call
- 1 - Terminating streaming call
- 2 - Terminating interactive call
- 3 - Terminating background call
- 4 - Terminating low priority signaling
- 5 - Terminating high priority signaling

**Example**

Use the following command to set Paging Cause value to 3 for paging due to GMM signaling without affecting cause values for other sources:

```
ranap paging-cause-ie gmm-signalling 3
```

Use the following command to suppress the Paging Cause IE from all Paging Requests to the RNC:
no ranap paging-cause-ie all

Either of the following commands will cause the Paging Cause IE to be included in Paging Requests with the default value for SM signaling without affecting the cause for other sources:

  ranap paging-cause-ie sm-signalling
  default ranap paging-cause-ie sm-signalling
**ranap signalling-indication-ie**

This command enables/disables the inclusion of the Signaling Indication IE in either or both the RAB Assignment Request and/or the Relocation Request RANAP messages.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
ranap signalling-indication-ie { rab-assignment-request [ relocation-request ] | relocation-request [ rab-assignment-request ] }

no ranap signalling-indication-ie

default ranap signalling-indication-ie
```

- **no**
  Sets the configuration so that the SGSN never includes the IE.

- **default**
  Resets the configuration to the default - the SGSN includes the IE in the messages if preconditions are met (see Usage section).

```bash
rab-assignment-request | relocation-request
```

Including one or both of these keywords configures what type of RANAP message will include the IE.

**Usage**
The command enables the operator to determine whether the signalling indication information element is included in either or both the RAB Assignment Request and Relocation Request messages during the PDP context setup procedure.

For this command configuration to work so that the IE is included, two preconditions must be met:

- Received QoS traffic class for the context must be interactive
- Received QoS has a signalling indication value as optimized

When an RNC receives this IE, the RNC assumes that the customer is using IMS signaling and allocates massive amounts of bandwidth, potentially causing cell congestion. This command enables the operator to determine the usage of this IE which provides the operator with additional session management control.

**Example**
Use the following command to include the signalling indication IE in the RAB Assignment Request:

```bash
ranap signalling-indication-ie rab-assignment-request
```
release-compliance

This command allows the SGSN to support 3GPP release 6 HSPA or release 7 HSPA+.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
release-compliance { pre-release-7 | release-7 }

default release-compliance
```

- **default**
  Returns the configuration to the default value, which is `release-7`.

- **pre-release-7**
  Identifies 3GPP Release 6 (R6) as the release the RNC is compliant with.

- **release-7**
  Identifies 3GPP Release 7 (R7) as the release the RNC is compliant with.

**Usage**

Use this command to match the 3GPP release support by the RNC. As the 3GPP releases each support differing data rate options - R6 supports HSPA and R7 supports HSPA+ - then selecting the compliance is a method of preforming data rate management on a per RNC basis.

**Example**

Enable HSPA fallback to R6 compliance:

```plaintext
release-compliance pre-release-7
```
reset-resource

This command enables the operator to control message length by configuring the number of IuConIDs sent in each RANAP Reset Resource messages.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
reset-resource max-iuconid-per-msg number

default reset-resource max-iuconid-per-msg

default
Resets the number of Iu connection Ids included in the Reset Resource messages. Default is 250.

max-iuconid-per-msg number
Sets the number of Iu connection Ids to be included in the Reset Resource messages.
number: Integer from 1 to 250.
Default: 250

Usage
Id numbers for each Iu connection are included in the RANAP Reset Resource messages. Including this potentially long stream of numbers can make the message very long. With this command, the operator can control the size of the messages by controlling the number of Id messages included in the messages.

Example
Limit the number of Iu connection Ids to 30:

reset-resource max-iuconid-per-msg 30
Chapter 174
Remote Address List Configuration Mode Commands

The Remote Address List Configuration Mode is used to configure address lists for the Remote Address-based Accounting feature on a per-context basis.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          radius accounting
          ip remote-address
          list number
            Remote Address List Config Mode
```
address

This command configures addresses for the Remote Address List.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```
address ip_address netmask subnet
noaddress ip_address netmask subnet
```

- **no**
  
  Removes a previously configured address.

```
address ip_address
```

  Specifies the IP address of the remote device.

  *ip_address* is the IPv4 address expressed in dotted-decimal notation.

```
netmask subnet
```

  Specifies the subnet mask of the remote device.

  *subnet* is the netmask expressed in dotted-decimal notation.

**Usage**

Use this command to configure remote address lists for use with the Remote Address-based accounting feature. A maximum of 10 address can be configured per list.

**Example**

The following command adds an IP address of 192.168.100.1 with a subnet mask of 255.255.255.0 to the list:

```
address 192.168.100.1 netmask 255.255.255.0
```
**end**

This command exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to change to the Exec mode.
exit

This command exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
Chapter 175
RoHC Profile Common Options Configuration Mode Commands

The RoHC Profile Common Options Configuration Mode is used to set timers that, upon expiration, release header compression contexts.

```
Exec Mode
configure
   Global Configuration Mode
      rohc-profile profile-name name
         RoHC Profile Configuration Mode
            common-options
               RoHC Profile Common Options Config Mode
```
delay-release-hc-context-timer

Sets a delay in releasing RoHC contexts allowing for context continuation during intra-gateway handoffs.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
delay-release-hc-context-timer  seconds
no delay-release-hc-context-timer
```

**Usage**
Use this command to set a delay in releasing a header compression context. This command is necessary when employing RoHC and mobility. Typically, when an RP connection is released, the header compression context is also released immediately. However, in mobility situations, such as intra-PDSN handoffs, the header compression context should be preserved. Adding a delay to cover the handoff time allows the context to be maintained.

A header compression context contains the compression/decompression configuration and statistics for the session.

**Example**
The following command sets the header compression release delay to 20 seconds:

```
delay-release-hc-context-timer 20
```
end

Exits the current mode and returns to the Exec Mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
```
exit
```

Usage
Return to the previous mode.
inactive-traffic-release-hc-context-timer

Set an inactivity timer that is checked when inactivity is detected on an SO67 A10 bearer connection with negotiated RoHC parameters. If the inactivity continues to the end of the configured time, the header compression context is released.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

inactive-traffic-release-hc-context-timer seconds

no inactive-traffic-release-hc-context-timer

Usage
Use this command to set a timer that is started upon detecting inactivity on the bearer channel. Upon expiry, the header compression context is released. Enable this feature to allow for efficient memory utilization.

Example
The following command sets the bearer channel inactivity timer to 60 seconds:

inactive-traffic-release-hc-context-timer 60
The RoHC Profile Compression Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor parameters. RoHC is not supported on GGSN.

**Important:** The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).
context-timeout

Context timeout in seconds.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

context-timeout seconds

default context-timeout

default
Returns the command to its default value.

seconds
Default: 20 seconds
The context timeout value in seconds. seconds must be an integer from 0 through 100.

Usage
Use this command to set the context timeout.

Example
The following command sets the context timeout to 10 seconds:

context-timeout-period 10
end

Returns the CLI prompt to the Exec mode.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits this configuration mode and returns to the previous mode.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
exit
```

Usage
Return to the previous mode.
ipid-history-size

The number of IP-IDs of previously sent packets to store. An IP ID is a 16-bit header field that stores IPv4 Identification information.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
ipid-history-size number

default ipid-history-size
```

**default**
Returns the command to its default value.

**number**
Default: 8
The number of IP IDs to store. `number` must be an integer from 1 through 32.

**Usage**
Use this command to set the number of IP IDs to store in the history.

**Example**
The following command sets the history size to 24 IP-IDs:

```
ipid-history-size 24
```
max-jitter-cd

The upper boundary of jitter expected on the communication channel between the compressor and decompressor.

**Product**

HSGW, PDSN

**Privilege**

Administrator

**Syntax**

```plaintext
max-jitter-cd num_ms
default max-jitter-cd
```

**default**

Returns the command to its default value.

- **num_ms**
  
  Default: 150
  
  The number of milliseconds for the maximum jitter setting. `num_ms` must be an integer from 0 through 999999999.

**Usage**

Use this command to set the maximum amount of jitter allowed on the communication channel between compressor and decompressor.

**Example**

The following command sets the jitter limit to 1000ms (1 second):

```
max-jitter-cd 1000
```
max-sliding-window

The width of the sliding window for W-LSB (Windows-based Least Significant Bits) encoded values.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
max-sliding-window size
```

```
default max-sliding-window
```

**Usage**
Use this command to set the size of the sliding window used to compute jitter for W-LSB encoded values.

**Example**
The following command sets the sliding window size to 500:

```
max-sliding-window 500
```
multiple-ts-stride

Enables or disables the use of repeated transmission of RTS_STRIDE for timer-based compression.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
[ no ] multiple-ts-stride

no
Disables the use of repeated transmission of RTS_STRIDE for time-based compression.

multiple-ts-stride
Enables the repeated transmission of RTS_STRIDE for timer-based compression.
```

**Usage**
Use this command to enable or disable a gateway’s ability to repeatedly transmit RTS_STRIDE for timer-based compression.
new-context-blocking-time

Time period in seconds for blocking the establishment of new contexts after the compressor has received a feedback reject.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

new-context-blocking-time seconds

default context-timeout

Usage
Use this command to set the context blocking time after the compressor has received a feedback reject.

Example
The following command sets the context blocking time to 10 seconds:

    new-context-blocking-time 10
num-pkts-ts

The number packets per RTP timestamp (TS).

Product
HSGW, PDSN

Privilege
Administrator

Syntax

 num-pkts-ts num_pkts

default num-pkts-ts

default
Returns the command to its default value.

 num_pkts
Default: 6
The number of packets for the timestamp. num_pkts must be an integer from 0 through 999.

Usage
Use this command to set the number of packets for each RTP timestamp (TS).

Example
The following command sets the number of packets per timestamp to 50:

 num-pkts-ts 50
num-pkts-u-mode

The number packets sent when operating in U-Mode (unidirectional mode).

**Product**
- HSGW, PDSN

**Privilege**
- Administrator

**Syntax**

```
num-pkts-u-mode num_pkts
default num-pkts-u-mode
```

**default**
Returns the command to its default value.

```
um_pkts
Default: 1
The number of packets sent in U-Mode. num_pkts must be an integer from 0 through 999.
```

**Usage**
Use this command to set the number of packets sent when in U-Mode.

**Example**
The following command sets the number of packets for U-Mode to 50:

```
um-pkts-u-mode 50
```
num-updates-ir

This command configures the number of IR (Initiation and Refresh state) updates.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
num-updates-ir num_pkts

default num-updates-ir
```

default

Returns the command to its default value.

```
um_pkts
```

Default: 4

The number of packets sent in U-Mode. num_pkts must be an integer from 0 through 999.

Usage

Use this command to set the number of packets sent when in U-Mode.

Example

The following command sets the number of packets for U-Mode to 50:

```
num-updates-ir 50
```
optimistic-repeats

For transition from the FO (First Order) to the SO (Second Order) state, the compressor should be confident that the decompressor has all the parameters needed to decompress according to a fixed pattern. The compressor obtains its confidence about decompressor status by sending several packets with the same information according to the lower compression state. If the decompressor receives any of these packets, it is in sync with the compressor. This command defines the number of repeated packets to send to the decompressor.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
optimistic-repeats num_pkts

default optimistic-repeats
```

**default**

Returns the command to its default value.

```
num_pkts
```

Default: 6

The number of packets to repeat with the same information to assure synchronization with the decompressor. `num_pkts` must be an integer from 0 through 10.

Usage

Use this command to set the number of packets to repeat to the decompressor to assure synchronization before transition states.

Example

The following command sets the number of repeated packets to 5:

```
optimistic-repeats 5
```
**rtp-sn-p**

The value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the decompressor derives the original value using a previously received value as reference (v_ref). The scheme is guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

\[ f(v_{\text{ref}}, k) = \left[ v_{\text{ref}} - p, v_{\text{ref}} + (2^k - 1) - p \right] \]

Where p is an integer.

**Product**

HSGW, PDSN

**Privilege**

Administrator

**Syntax**

```
  rtp-sn-p  p_value
```

```
default rtp-sn-p
```

- **default**
  - Returns the command to its default value.

- **p_value**
  - Default: 6
  - The number to use for the value of p in the RTP SN calculation. p_value must be an integer from 0 through 999.

**Usage**

Use this command to set the value to use for p when performing the RTP SN calculation.

**Example**

The following command sets the value of p to 100:

```
rtp-sn-p 100
```
**rtp-sn-p-override**

Allow an override of p in RTP SN calculation. This is disabled by default.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
[ default | no ] rtp-sn-p-override
```

- **default**
  Returns the command to its default value of disabled.

- **no**
  Disables overriding p in RTP SN calculation.

**Usage**

Use this command to enable an override of p in RTP SN calculation.

**Example**

The following command enables the override of p in the RTP SN calculation:

```
rtp-sn-p-override
```
rtp-time-stride

This command sets the time interval used for one TS (RTP Time Stamp) stride. This is used when timer-based encoding is enabled.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

    rtp-time-stride  num_ms

    default  rtp-time-stride

---------

default

    Returns the command to its default value.

---------

num_ms

    Default: 20
    The number of milliseconds to use for TS_STRIDE. num_ms must be an integer from 0 through 999999999.

---------

Usage

    Use this command to set the length of the TS_STRIDE in milliseconds.

---------

Example

    The following command sets TS_STRIDE to 100ms:

        rtp-time-stride 100
rtp-ts-deviation

This command sets the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```plaintext
rtp-ts-deviation percentage
```

```plaintext
default rtp-ts-deviation percentage
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to its default value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 25</td>
</tr>
<tr>
<td>Specifies the maximum percentage of deviation allowed for input RTP packets for timer-based compression. percentage must be an integer value from 0 through 100.</td>
</tr>
</tbody>
</table>

Usage
Use this command to set the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

Example
The following command sets the time increment to 1000:

```plaintext
rtp-ts-deviation 25
```
**rtp-ts-stride**

Amount by which TS (RTP time stamp) is incremented. This is used for Scaled RTP TS encoding.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
rtp-ts-stride num_ms
```

```
default rtp-ts-stride
```

**default**

Returns the command to its default value.

```
num_ms
```

Default: 160
The number of milliseconds to use incrementing TS. `num_ms` must be an integer from 0 through 999999999.

**Usage**

Use this command to set the amount by which TS is incremented for Scaled RTP TS encoding.

**Example**

The following command sets amount by which TS is incremented to 100ms:

```
rtp-ts-stride 100
```
**sliding-window-ts**

**Description** The sliding window used to compute jitter.

**Product** HSGW, PDSN

**Privilege** Administrator

**Syntax**

```
sliding-window-ts size
```

default sliding-window-ts

**default**

Returns the command to its default value.

```
size
```

Default: 4
Set the size of the sliding window. `size` must be an integer from 1 through 1000.

**Usage**

Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

**Example**

The following command sets the sliding window size to 500:

```
sliding-window-ts 500
```
The total jitter experienced after compression for IPV4.

Product
HSGW, PDSN

Privilege
Administrator

Syntax
```
total-jitter-ipv4 time
```
```
default total-jitter-ipv4
```

**default**
Returns the command to its default value.

- **time**
  Default: 270
  Specifies the time interval to use in milliseconds. `time` must be an integer from 0 through 999999999.

**Usage**
Use this command to set the jitter limit after compression.

**Example**
The following command sets the jitter after compression limit to 900ms:
```
total-jitter-ipv4 900
```
**total-jitter-ipv6**

The total jitter experienced after compression for IPV6.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
total-jitter-ipv6 time
```

```
default total-jitter-ipv6
```

**default**

Returns the command to its default value.

```
time
```

Default: 580
Specifies the time interval to use in milliseconds. `time` must be an integer from 0 through 999999999.

**Usage**

Use this command to set the jitter limit after compression.

**Example**

The following command sets the jitter after compression limit to 900 ms:

```
total-jitter-ipv6 900
```
unimode-timeout-to-fo-state

The time period in seconds before falling back to the FO (First Order) state.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

unimode-timeout-to-fo-state num_ms

default unimode-timeout-to-fo-state

default

Returns the command to its default value.

num_ms

Default: 3
Timeout period in seconds. num_ms must be an integer from 0 through 10.

Usage

Use this command to set the timeout before falling back to the FO state when in Unimode.

Example

The following command sets the fall back timeout to 3 seconds:

unimode-timeout-to-fo-state 3
unimode-timeout-to-ir-state

The time period in seconds before falling back to the IR (Initiation and Refresh) state.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

unimode-timeout-to-ir-state  num_ms

default unimode-timeout-to-ir-state

default
Returns the command to its default value.

num_ms
Default: 5
Timeout period in seconds. num_ms must be an integer from 0 through 20.

Usage
Use this command to set the timeout before falling back to the IR state when in Unimode.

Example
The following command sets the fall back timeout to 3 seconds:

unimode-timeout-to-ir-state 3
use-calculated-rtp-time-stride

This command overrides the configured value of rtp-time-stride with a calculated value.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default | no ] use-calculated-rtp-time-stride

default
Returns the command to its default value of enabled.

no
Disables the use of calculated RTP time stride override.

Usage
This command overrides the configured value of rtp-time-stride with a calculated value.

Example
The following command overrides the configured value of rtp-time-stride.

use-calculated-rtp-time-stride
use-calculated-rtp-ts-stride

This command overrides the configured value of rtp-ts-stride with a calculated value.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```plaintext
[ default | no ] use-calculated-rtp-ts-stride
```

default
Returns the command to its default value of enabled.

no
Disables the use of calculated RTP TS time stride override.

Usage
This command overrides the configured value of rtp-ts-stride with a calculated value.

Example
The following command overrides the configured value of rtp-ts-stride.

```
use-calculated-rtp-ts-stride
```
**use-ipid-override**

Enable and disable overriding the IP-ID (IPv4 Identification header field).

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
[ default | no ] use-ipid-override
```

- **default**
  Returns the command to its default value of disabled.

- **no**
  Disables the IP-ID override.

**Usage**

Use this command to enable overriding the IP-ID.

**Example**

The following command enables the IP-ID override feature:

```
use-ipid-override
```

The following command disables the IP-ID override feature:

```
o use-ipid-override
```

The following command also disables the IP-ID override feature:

```
default use-ipid-override
```
use-optimized-talkspurt

Disable and enable the use of optimized talkspurt.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default | no ] use-optimized-talkspurt

---

default
Returns the command to its default value of enabled.

---

no
Disable the use of optimized talkspurt.

Usage
Use this command to enable and disable the use of optimized talkspurt

Example
The following command enables the use of optimized talkspurt:

use-optimized-talkspurt

The following command disables the use of optimized talkspurt:

no use-optimized-talkspurt
use-optimized-transience

Enable or disable the use of optimized transience.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default | no ] use-optimized-transience

---

**default**

Returns the command to its default value of enabled.

---

**no**

Disables the use of optimized transience.

---

Usage

Use this command to enable or disable the use of optimized transience.

---

Example

The following command enables the use of optimized transience.

```
use-optimized-transience
```

The following command disables the use of optimized transience.

```
no use-optimized-transience
```
use-timer-based-compression

Enables timer-based compression of the RTP time stamp (TS) at the compressor.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
[ default | no ] use-timer-based-compression
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Returns the command to its default value of enabled.</td>
</tr>
<tr>
<td>no</td>
<td>Disables the use of timer-based compression.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable or disable the use of timer-based compression.

**Example**

The following command enables the use of timer-based compression.

```
use-timer-based-compression
```

The following command disables the use of timer-based compression.

```
no use-timer-based-compression
```
use-uncomp-profile

Uses the Uncompressed Profile (0x0000) if required at the compressor.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[default | no ] use-uncomp-profile

default
Returns the command to its default value of disabled.

no
Disables the use of the Uncompressed Profile.

Usage
Use this command to enable or disable the use of the Uncompressed Profile.

Example
The following command enables the use of the Uncompressed Profile.

use-uncomp-profile

The following command disables the use of the Uncompressed Profile.

no use-uncomp-profile
Chapter 177
RoHC Profile Configuration Mode Commands

The RoHC Profile Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor and Decompressor parameters. The profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured. RoHC is not supported on GGSN.

Important: The availability of commands, keywords and variables in this mode is dependent on platform type, product version, and installed license(s).
common-options

Enters the RoHC Profile Common Options Configuration Mode where inactivity and delay timers are set to support dynamic header compression contexts and context preservation during handoffs.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default ] common-options

default
Reset all parameters in the RoHC Profile Common Options Configuration Mode to default values.

Usage
Use this command to enter the RoHC Profile Common Options Configuration Mode where parameters for maintaining header compression contexts and inactivity timers can be configured. Entering this command results in the following prompt:
[context_name]host(config-rohcp-profile-<profile_name>-common)#
RoHC Profile Common Options Configuration Mode commands are defined in the RoHC Profile Common Options Configuration Mode Commands chapter.
compression-options

Enters the RoHC Profile Compression Options Configuration Mode allowing configuration of options applied during RoHC compression for the current RoHC profile.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default ] compression-options

default
Reset all options in the RoHC Profile Compression Configuration Mode to their default values.

Usage
Use this command to enter RoHC Profile Compression Configuration Mode to set the compression options that are used for subscriber sessions using the current RoHC profile. Entering this command results in the following prompt:
[context_name]host(config-rohcprofile-<profile_name>-comp)#
RoHC Profile Compression Options Configuration Mode commands are defined in the RoHC Profile Compression Configuration Mode Commands chapter.

Example
The following command enters RoHC Profile Compression Options Configuration Mode:

    compression-options

The following command sets all compression options to their default values:

    default compression-options
decompression-options

Enters the RoHC Profile Decompression Options Configuration Mode allowing configuration of options applied during RoHC decompression for the current RoHC profile.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
[default ] decompression-options
```

**default**
Reset all options in the RoHC Profile Decompression Options Configuration Mode to their default values.

Usage
Use this command to enter RoHC Profile Decompression Options Configuration Mode to set the decompression options used for subscriber sessions using the current RoHC profile. Entering this command results in the following prompt:

```
[context_name]host(config-rohcprofile-<profile_name>-decomp)#
```

RoHC Profile Decompression Options Configuration Mode commands are defined in the RoHC Profile Decompression Configuration Mode Commands chapter.

Example
The following command enters RoHC Profile Decompression Options Configuration Mode:

```
decompression-options
```

The following command sets all decompression options to their default values:

```
default decompression-options
```
end

Returns the CLI prompt to to the Exec mode.

Product
HSGW, PDSN

Privilege
Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
**exit**

Exits this configuration mode and returns to the previous mode.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**
```
exit
```
Chapter 178
RoHC Profile Decompression Configuration Mode
Commands

The RoHC Profile Decompression Configuration Mode is used to configure RoHC (Robust Header Compression) Decompressor parameters.

**Important:** The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).
accept-delayed-pkts

Accepts delayed packets

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default ] accept-delayed-pkts

default
Returns the command to its default value of disabled.

Usage
This command helps reduce packet loss during context repair.

Example
Use the following command to enable the system to accept delayed packets:

accept-delayed-pkts
context-timeout

Ensures that no expired contexts are used for data compression.

Product
HSGW, PDSN

Privilege
Administrator

Syntax
context-timeout  seconds

default  ]  context-timeout

default
Returns the command to its default value.

seconds
Default: 20 seconds
The context timeout value in seconds. seconds must be an integer from 0 through 100.

Usage
The RoHC stack should periodically clean up expired contexts and release memory in case there is no data activity for the call on this context. The context cleanup period is internally calculated to be set to half of the context-timeout value. This will ensure that no expired contexts are used for data compression.

Example
The following command sets the context-timeout parameter to 30 seconds:

context-timeout  30
**crc-errors-fo**

This command sets the limits for when a NACK message is sent when in the FO (First Order) state. A NACK is sent when out of a specified number of packets a specified number of them have CRC errors.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
crc-errors-fo-k num_errors

crc-errors-fo-n num_packts

default crc-errors-fo-k

default crc-errors-fo-n
```

---

```
default
```

Returns the command to its default value.

```
crc-errors-fo-k num_errors
```

Default: 1
The number of received packets within a specified number of received packets that triggers the sending of a NACK. `num_errors` must be an integer from 1 through 10.

**Important:** `num_errors` must be less than or equal to the value specified with the `crc-errors-fo-n` command.

```
crc-errors-fo-n num_packts
```

Default: 1
The number of packets to check for CRC errors. `num_packts` must be an integer from 1 through 10.

---

**Usage**

Use this command to set the parameters that trigger sending a NACK message when in the FO state.

---

**Example**

To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the FO state, use the following commands:

```
crc-errors-fo-k 4
crc-errors-fo-n 10
```


crc-errors-so

This command sets the limits for when a NACK message is sent when in the SO (Second Order) state. A NACK is sent when out of a specified number of packets a specified number of them have CRC errors.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

- `crc-errors-so-k num_errors`
- `crc-errors-so-n num_packets`
- `default crc-errors-so-k`
- `default crc-errors-so-n`

  **default**
  Returns the command to its default value.

  `crc-errors-so-k num_errors`
  Default: 1
  The number of received packets within a specified number of received packets that triggers the sending of a NACK. `num_errors` must be an integer from 0 through 10.

  **Important**: `num_errors` must be less than or equal to the value specified with the `crc-errors-so-n` command.

  `crc-errors-so-n num_packets`
  Default: 1
  The number of packets to check for CRC errors. `num_packets` must be an integer from 1 through 10.

**Usage**
Use this command to set the parameters that trigger sending a NACK message when in the SO state.

**Example**
To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the SO state, use the following commands:

```
crc-errors-so-k 4
```
```
**end**

Returns the CLI prompt to to the Exec mode.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**
```plaintext
dec
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the this configuration mode and returns to the previous mode.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

exit

Usage
Return to the previous mode.
nack-limit

Sets the number of unsuccessful decompressions allowed before a NACK is sent.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```
nack-limit limit
default nack-limit
```

- **Default**
  Returns the command to its default value.

- **limit**
  Default: 0
  Specifies the number of unsuccessful decompressions allowed. *limit* must be an integer from 0 through 20.

**Usage**
Use this command to set the maximum number of unsuccessful decompressions before a NACK message is sent.

**Example**
The following command sets the number of unsuccessful decompressions allowed to 10:

```
nack-limit 10
```
optimistic-mode-ack

When this is enabled, if a type 2 IR-DYN packet is successfully decompressed, an optional ACK is sent in U-mode.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default | no ] optimistic-mode-ack

default
Returns the command to its default value of enabled.

no
Disables the sending of the optional ACK.

Usage
Use this command to enable and disable the sending of an optional ACK in U-mode when a type 2 IR-DYN packet is successfully decompressed.

Example
To enable the sending of the optional ACK, enter the following command:

   optimistic-mode-ack

To disable the sending of the optional ACK, enter the following command:

   no optimistic-mode-ack
**optimistic-mode-ack-limit**

When enabled, this command sets the number of packets to send ACKs for.

**Product**
HSGW, PDSN

**Privilege**
Administrator

**Syntax**

```plaintext
optimistic-mode-ack-limit num_pkts

default optimistic-mode-ack-limit
```

- **default**
  Returns the command to its default value.

- **num_pkts**
  Default: 3
  The number of packets to send ACKs for. `num_pkts` must be an integer from 0 through 20.

**Usage**
Use this command to set the number of packets to send the optional ACK for when a type 2 IR-DYN packet is successfully decompressed.

**Example**
Enter the following command to set the number of packets to send and ACK for to 6:

```
optimistic-mode-ack-limit 6
```

Use the following command to set the number of packets to send an ACK for back to the default of 3:

```
default optimistic-mode-ack-limit
```
piggyback-wait-time

The time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
piggyback-wait-time msecs
```

```
default piggyback-wait-time
```

```
default
Returns the command to its default value.
```

```
msecs
Default: 80ms
Specifies the time in milliseconds to wait for a feedback packet to be picked up. $msecs$ must be an integer value from 0 through 1000.
```

Usage
Use this command to set the time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

Example
The following command sets the wait time to 120 ms:

```
piggyback-wait-time 120
```
preferred-feedback-mode

Specifies the preferred feedback mode to use between the compressor and the decompressor

Product
HSGW, PDSN

Privilege
Administrator

Syntax

preferred-feedback-mode { bidirectional-optimistic | bidirectional-reliable | unidirectional }

default preferred-feedback-mode

default
Default: bidirectional-optimistic
Returns the command to its default setting.

bidirectional-optimistic
This mode is similar to the Unidirectional mode, with the exception of a feedback channel used to send error recovery requests from the decompressor to compressor.

bidirectional-reliable
Reliable mode makes extensive use of a feedback channel to avoid packet loss from context invalidation. A secure reference model is used instead of the optimistic approach used in the other modes. With the secure reference model, the confidence of the compressor depends on acknowledgements from the decompressor for every context updating packet. Periodically the compressor sends context updating packets repeatedly until an acknowledgement is received from the decompressor.

unidirectional
Packets are sent in only one direction, from the compressor to the decompressor.

Usage
Use this command to specify the preferred feedback method to use between the compressor and the decompressor for the current RoHC profile.

Example
Use the following command to set the preferred feedback mode to bidirectional-reliable:

preferred-feedback-mode bidirectional-reliable
rtp-sn-p

The value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for
header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the
field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the
decompressor derives the original value using a previously received value as reference (v_ref). The scheme is
guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

\[ f(v_{\text{ref}}, k) = [v_{\text{ref}} - p, v_{\text{ref}} + (2^k - 1) - p] \]

Where p is an integer.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

rtp-sn-p value

default rtp-sn-p

default

Returns the command to its default value.

value

Default:
Specifies the number to use for the value of p in the RTP SN calculation. value must be an integer from 0 through 999.

Usage

Use this command to set the value to use for p when performing the RTP SN calculation.

Example

The following command sets the RTP Sequence Number integer “p” value to 100:

rtp-sn-p 100
rtp-sn-p-override

Allow an override of p in RTP SN calculation. This is disabled by default.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

\[
\text{[ default | no ] rtp-sn-p-override}
\]

- **default**
  Returns the command to its default value of disabled.

- **no**
  Disables overriding p in RTP SN calculation.

Usage
Use this command to allow an override of p in RTP SN calculations.

Example
The following command enables the override of p in the RTP SN calculation:

```
rtp-sn-p-override
```
sliding-window-ts

Computes jitter as described in RFC 3095,[4.5.4]

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
sliding-window-ts size
```

default sliding-window-ts

```
default
Returns the command to its default value.
```

```
size
Default: 4
Set the size of the sliding window. size must be an integer from 1 through 1000.
```

Usage
Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

Example
The following command sets the sliding window size to 500:

```
sliding-window-ts 500
```
**use-clock-option**

Controls usage of RoHC clock option. The clock option informs the compressor of the clock resolution of the decompressor. This is needed to allow the compressor to estimate the jitter introduced by the clock of the decompressor when doing timer-based compression of the RTP timestamp.

**Product**

HSGW, PDSN

**Privilege**

Administrator

**Syntax**

```
[ default | no ] use-clock-option
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disable use of the RoHC clock option.

**Usage**

Use this command to enable and disable the use of the RoHC clock option.

**Example**

The following command enables RoHC clock option usage:

```
use-clock-option
```

The following command disables RoHC clock option usage:

```
no use-clock-option
```
use-crc-option

Controls usage of the RoHC crc option. The CRC option contains an 8-bit CRC computed over the entire feedback payload, without the packet type and code octet, but including any CID fields.

Syntax

[ default | no ] use-crc-option

- **default**
  - Returns the command to its default value of enabled.

- **no**
  - Disable use of the CRC option.

Usage

Use this command to enable and disable the use of the RoHC CRC option.

Example

The following command enables RoHC CRC option usage:

```
use-crc-option
```

The following command disables RoHC CRC option usage:

```
no use-crc-option
```
use-feedback

Controls use of the feedback channel. A feedback channel sends error recovery requests and (optionally) acknowledgments of significant context updates from the decompressor to the compressor.

Product
HSGW, PDSN

Privilege
Security Administrator, Administrator

Syntax

[ default | no ] use-feedback

default
Returns the command to its default value of disabled.

no
Disable use of the feedback channel.

Usage
Use this command to enable and disable the use of the RoHC feedback channel.

Example
The following command enables RoHC feedback channel usage:

    use-feedback

The following command disables RoHC feedback channel usage:

    no use-feedback
use-jitter-option

Controls usage of RoHC jitter option. The jitter option allows the decompressor to report the maximum jitter it has observed.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

[ default | no ] use-jitter-option

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to its default value of enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable use of the jitter option.</td>
</tr>
</tbody>
</table>

Usage
Use this command to enable and disable the use of the RoHC jitter option.

Example
The following command enables RoHC jitter option usage:

```
use-jitter-option
```

The following command disables RoHC jitter option usage:

```
no use-jitter-option
```
use-reject-option

Controls usage of RoHC reject option. The reject option informs the compressor that the decompressor does not have sufficient resources to handle the flow.

Product
HSGW, PDSN

Privilege
Administrator

Syntax

```
[ default | no ] use-reject-option
```

- **default**
  Returns the command to its default value of disabled.

- **no**
  Disable use of the reject option.

Usage
Use this command to enable and disable the use of the RoHC reject option.

Example
The following command enables RoHC reject option usage:

```
use-reject-option
```

The following command disables RoHC reject option usage:

```
no use-reject-option
```
use-sn-not-valid-option

Controls usage of the RoHC SN not valid option. The sn-not-valid option indicates that the SN of the feedback is not valid. A compressor must not use the SN of the feedback to find the corresponding sent header when this option is present.

Product  
HSGW, PDSN

Privilege  
Administrator

Syntax

```
[ default | no ] use-sn-not-valid-option
```

- **default**  
  Returns the command to its default value of enabled.

- **no**  
  Disable use of the sn-not-valid option.

Usage

Use this command to enable and disable the use of the RoHC sn not valid option.

Example

The following command enables RoHC sn not valid option usage:

```
use-sn-not-valid-option
```

The following command disables RoHC sn not valid option usage:

```
no use-sn-not-valid-option
```
use-sn-option

Controls usage of RoHC sn option. The sn option provides 8 additional bits of SN (Sequence Number. Usually RTP Sequence Number.)

Product

HSGW, PDSN

Privilege

Administrator

Syntax

[ default | no ] use-sn-option

default

Returns the command to its default value of enabled.

no

Disable use of the sn option.

Usage

Use this command to enable and disable the use of the RoHC sn option.

Example

The following command enables RoHC sn option usage:

use-sn-option

The following command disables RoHC sn option usage:

no use-sn-option
Chapter 179
Route-map Configuration Mode Commands

The Route-Map Configuration sub-mode is used for the OSPFv2 and BGP-4 routing protocols. This mode includes commands that configure matching rules and set actions to perform on matched routes.

```
Exec Mode
  configure
  Global Configuration Mode
    context name
      Context Configuration Mode
        route-map name { deny | permit }
          Route-map Configuration Mode
```

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

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the context configuration mode and returns to the global configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the global configuration mode.
match as-path

Match an AS path access list

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
match as-path AS_list
no match interface AS_list
```

Usage
This command is used for BGP-4 routing to specify an AS path access list to be matched. Refer to the `ip as-path access-list` command for more information.

Example
To match entries in an AS path access list named ASlist1, enter the following command:
```
macth as-path ASlist1
```
match interface

Specifies the next-hop interface name of a route to be matched.

Product
All

Privilege
Security Administrator, Administrator

Syntax

match interface interface-name
no match interface interface-name

Usage
Use this command to specify the next hop interface name for routes to be matched.

Example
To match routes that have the next hop interface specified as Interface123, enter the following command:
match interface Interface123
To disable matching routes that have the next hop interface specified as Interface123, enter the following command:
no match interface Interface123
match ip address

This command matches routes with entries in a route-access-list or prefix-list.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
match ip address {prefix-list|route-access-list} list_name
no match ip address {prefix-list|route-access-list} list_name
```

- **no**
  Disable matching from the specified prefix list or route access list.

- **prefix-list**
  This command matches any routes with entries in a prefix-list.

- **route-access-list**
  This command matches any routes with entries in a route-access-list

- **list_name**
  The name of the IP prefix list or IP route access-list. This variable can be a string from 1 to 63 alphanumeric characters in length.

Usage

Use this command to match routes specified in a route-access-list or prefix-list.

Example

To match routes that are specified in a prefix list named `Prefix100`, enter the following command:

```bash
match ip address prefix-list Prefix100
```

To disable matching routes that are specified in a prefix list named `Prefix100`, enter the following command:

```bash
no match ip address prefix-list Prefix100
```
**match ip next-hop**

This command matches next-hop IP addresses with entries in specified standard prefix-list or route-access-list.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
match ip address next-hop {prefix-list | route-access-list} list_name
no match ip address next-hop {prefix-list | route-access-list} list_name
```

- **prefix-list**
  This command matches any routes that have a next-hop router address that has an entry in the specified prefix list.

- **route-access-list**
  This command matches any routes that have a next-hop router address that has an entry in the specified route-access-list.

- **list_name**
  The name of the IP prefix-list or IP route-access-list. This variable is a string from 1 through 63 alphanumeric characters in length.

**Usage**

Use this command to match next-hop IP addresses that have entries in the specified prefix-list or route-access-list.

**Example**

To match next-hop addresses with entries in a prefix-list named *Prefix100*, enter the following command:
```
match ip address next-hop prefix-list Prefix100
```

To disable matching next-hop addresses with entries in a prefix-list named *Prefix100*, enter the following command:
```
no match ip address next-hop prefix-list Prefix100
```
match metric

This command matches routes that have the specified route metric.

Product
All

Privilege
Security Administrator, Administrator

Syntax

match metric metric_value
no match metric metric_value

no
Disables matching of the specified route metric.

metric_value
This is the route metric to match. This must be an integer ranging from 0 through 4294967295.

Usage
Use this command to match routes that have the specified route metric.

Example
To match routes with the route metric of 1200, enter the following command:
match metric 1200
To disable matching routes with a route metric of 1200, enter the following command:
no match metric 1200
match origin

This command matches the origin code learned from BGP. This command is for route maps that are used with BGP routing only.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
match origin {egp | igp | incomplete}
no match origin {egp | igp | incomplete}
```

- **no**
  Disables matching of the origin code.

- **egp**
  Match origins learned from the External Gateway Protocol (EGP)

- **igp**
  Match origins learned from the local Interior Gateway Protocol (IGP)

- **incomplete**
  Match origins with unknown heritage.

Usage

Use this command to match origin codes for BGP routing.

Example

To match origin codes learned from EGP, enter the following command:

```
match origin egp
```
**match route-type external**

Match external OSPF routes of the specified type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
match route-type external { type-1 | type-2 }
```

```
no match route-type external { type-1 | type-2 }
```

**type-1**

Only match type-1 external routes.

**type-2**

Only match type-2 external routes.

**Usage**

Use this command to match external routes of a specific type.

**Example**

The following command matches all external routes that are type-2:
```
match route-type external type-2
```

The following command disables matching external routes that are type-2:
```
no match route-type external type-2
```
match tag

This command matches routes with the specified route tag value.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
match tag tag_value
no match tag tag_value
``` 

```plaintext
no
```

Disable matching routes with the specified route tag value.

```plaintext
tag_value
```

The route tag value to match. This must be an integer from 0 through 4294967295.

**Usage**

Use this command to match routes that have the specified route tag value.

**Example**

Use the following command match routes that have a route tag value of 1234:

```plaintext
match tag 1234
```

Use the following command to disable matching routes that have a route tag value of 1234:

```plaintext
no match tag 1234
```
**set as-path**

Modify an AS path for a route by adding the specified AS numbers to the front of the path.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Syntax**

```
set as-path prepend \texttt{ASN}
no set as-path prepend \texttt{ASN}
```

**no**

Disable prepending the AS path. Any previously set prepends are removed.

**prepend**

Prepends the autonomous system path.

**ASN**

AS number(s) to be prepended to the AS path. You can specify up to 16 different AS numbers to be prepended in the order specified. Each AS number must be separated by a space. \texttt{ASN} must be an integer from 1 through 65535.

**Usage**

Use this command to add up to 16 specified AS numbers to the front of the AS path.

**Example**

The following command prepends the AS numbers 100, 200, and 1000 to matching AS paths:

```
set as-path prepend 100 200 1000
```
**set ip next-hop**

Set the IP address that is applied as the next hop for routes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
set ip next-hop ip_address
no set ip next-hop ip_address
```

**Usage**

Use this command to set the IP address that is used as the next hop for routes.

**Example**

To set the next hop for routes to the IP address `192.168.2.100`, use the following command:

```
set ip next-hop 192.168.2.100
```

To disable setting the next hop for routes to the IP address `192.168.2.100`, use the following command:

```
no set ip next-hop 192.168.2.100
```
set metric

This command sets the route metric for matched routes to the specified value.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
set metric metric_value
no set metric metric_value
```

*metric_value*

This is the metric value that is set for routes. This must be an integer from 1 through 4294967295.

**Usage**
Use this command to set the route metric for matched routes.

**Example**

To set the route metric to 12345, use the following command;
set metric 12345

To disable setting the route metric to 12345, enter the following command;
no set metric 12345
set metric-type

This command sets the route metric type to either Type-1 or Type-2 in the AS-external-LSA.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
set metric-type {type-1|type-2}
no set metric-type {type-1|type-2}
```

- **type-1**
  Set the route metric to external type-1.

- **type-2**
  Set the route metric to external type-2

**Usage**
Use this command to set the route metric to either external type-1 or external type-2.

**Example**
To set the route metric to type-1, enter the following command:
```
set metric type-1
```
To disable setting the metric to type, enter the following command:
```
no set metric type-1
```
set origin

This command sets the BGP origin code to the specified value. This command is for route maps that are used with BGP routing only.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

```
set origin {egp | igp | incomplete}
no set origin {egp | igp | incomplete}
```

- **no**
  Disables setting the origin code.

- **egp**
  Set the origin code to specify that the path is from a remote External Gateway Protocol (EGP) system.

- **igp**
  Set the origin code to specify that the path is from a local Interior Gateway Protocol (IGP) system.

- **incomplete**
  Set the origin code to specify that the path is from an unknown system.

Usage
Use this command to set a specified origin code for BGP.

Example
To the origin code to EGP, enter the following command:

```
set origin egp
```
**set tag**

This command sets the route tag value for matched routes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
set tag tag_value
no set tag tag_value
```

**Usage**

Use this command to set the route tag value that is applied to all matched routes.

**Example**

To set the route tag value to 12345, enter the following command:
```
set tag 12345
```

To disable setting the route tag value to 12345, enter the following command:
```
no set tag 12345
```
set weight

Set the weight in the routing table for matching routes to the specified value.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
set weight value
no set weight value
```

- **no**
  Disable setting the routing weight value.

- **value**
  The weight in the routing table to assign. must be an integer from 1 through 4294967295.

**Usage**
Use this command to set the routing table weight on matched routes.

**Example**
The following command sets the routing table weight for matched routes to 1000:
```
set weight 1000
```
Chapter 180
RS-232 Port Configuration Mode Commands

The RS-232 Port Configuration Mode is used to manage the RS-232 ports on the SPIO cards.
default

Restores the port’s default speed and communication mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
default {preferred slot | terminal {all | databits | flowcontrol | parity | speed | stopbits}}
```

```
preferred slot
```
Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port.

```
terminal { all | databits | flowcontrol | parity | speed | stopbits }
```

Sets the terminal settings for the rs-232 port to their default settings.

- **all**: Restore all settings to their default values.
- **databits**: Restore the databits setting to its default value of 8.
- **flowcontrol**: Restore the flowcontrol setting to its default value of none.
- **parity**: Restore the parity setting to its default value of none.
- **speed**: Restore the speed setting to its default value of 9600.
- **stopbits**: Restore the stopbits setting to its default value of 1.

Usage

Restores port-level parameters to their default values.

Example

The following command restores all terminal settings to their default values:

```
default terminal all
```
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```text
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the port configuration mode and returns to the global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
  exit

Usage
Return to the global configuration mode.
preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery.

Default: non-revertive operation

Product

PDSN, FA, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```plaintext
preferred slot slot#
no preferred slot slot#

no
Disables revertive, or auto-recovery, operation for selected port.

slot#
Identifies the physical chassis slot where the SPIO card is installed.
```

Usage

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically. Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port. This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the LC in slot 17 while ports 5 through 8 are “preferred” on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Important: This command is not supported on all platforms.

Example

```
preferred slot 24
```
**snmp trap link-status**

Enables/disables the generation of an SNMP trap for link status changes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
   snmp trap link-status
   no snmp trap link-status
```

```
   no
```

Disables the sending of traps for link status changes.

**Usage**
Enable link status change traps when a monitoring facility can use the information or if there are troubleshooting activities are in progress.

**Example**

```
   snmp trap link-status
   no snmp trap link-status
```
**terminal**

Configures the console port on the SPIO.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
terminal { carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware | none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 | 9600 } | stopbits { 1 | 2 } }
```

---

**carrierdetect { off | on }**

Default: none

Specifies whether or not the console port is to use carrier detect when connecting to a terminal.

---

**databits { 7 | 8 }**

Default: 8

Specifies the number of data bits used to transmit and receive characters.

---

**flowcontrol { hardware | none }**

Default: none

Specifies how the flow of data is controlled between the SPIO and a terminal.

---

**parity { even | none | odd }**

Default: none

Specifies the type of error checking used on the port.

- **even** - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.
- **none** - Disables error checking.
- **odd** - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

---

**speed { 115200 | 19200 | 38400 | 57600 | 9600 }**

Default: 9600

Specifies the flow of data in bits per second between the console port and terminal.

---

**stopbits { 1 | 2 }**

Default: 1

Specifies the number of stop bits between each transmitted character.

---

**Usage**

Sets the SPIO’s console port parameters for communication with the terminal device.
Example
The following command sets the SPIO’s console port. The terminal must support these values.
```bash
terminal carrierdetect off databits 7 flowcontrol hardware parity even speed 115200 stopbits 1
```
Chapter 181
Rulebase Configuration Mode Commands

The Rulebase Configuration Mode is used to create and manage Active Charging Service Rulebase configurations.

```
Exec Mode

active-charging
  service name

ACS
  Configuration
  Mode

rulebase name

Rulebase
  Configuration
  Mode
```

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

This command configures the action priority for a ruledef / group-of-ruledefs in the rulebase.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

no action priority action_priority

no
Removes the previously configured action priority from this rulebase.

priority action_priority
Specifies a priority for the specified ruledef / group-of-ruledefs in this rulebase.
The priority controls the ordering of the instance of the CLI command. Lower numbered priorities are
examined first. Up to 2048 instances may be configured, totaled among all rulebases.
action_priority must be an integer from 1 through 65535.

dynamic-only
Default: disabled
Enables matching of dynamic rules with static rules for this action priority on a flow.
The dynamic-only option causes the configuration to be defined, but not enabled. If enabled, the action
associated with this option will not be matched against a flow until it is enabled from a dynamic charging
interface like Gx. Gx can disable or enable this action entry in the rulebase using Gx messages.

static-and-dynamic
Default: enabled
The static-and-dynamic option causes the configuration to be defined and enabled, and allows a dynamic
protocol (such as, the Gx-interface) to disable or re-enable the configuration.

Important: When R7 Gx is enabled, “static-and-dynamic” rules behave exactly like “dynamic-only” rules. I.e.
they must be activated explicitly by the PCRF. When Gx is not enabled, “static-and-dynamic” rules behave exactly like
static rules.

timedef timedef_name

Important: This keyword is only available in StarOS 8.1 and StarOS 9.0 and later releases.

Associates the specified time definition with the ruledef/group-of-ruledefs. Timedefs enable
activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only
when they are active.
timedef_name must be the name of a timedef, and must be an alpha and/or numeric string of 1 through 63 characters in length. A timedef can be used with several ruledefs/group-of-ruledefs. When a packet is received, and a ruledef/group-of-ruledefs is eligible for rule matching, if a timedef is associated with the ruledef/group-of-ruledefs, before rule matching, the packet-arrival time is compared with the timeslots configured in the timedef. If the packet arrived in any of the timeslots configured in the associated timedef, rule matching is undertaken, else the next ruledef/group-of-ruledefs is considered.

**Important:** The time considered for timedef matching is the system’s local time.

ruledef ruledef_name
Assigns the specified ruledef to this rulebase.
ruledef_name must be the name of an existing ruledef, and must be an alpha and/or numeric string of 1 through 63 characters in length.
If the specified ruledef does not exist, there will be no ruledef triggers for this action priority within this rulebase.

**Important:** If the ruledef specified here is deleted or is not configured, the system accepts it without applying any ruledef under current rulebase for this action priority.

group-of-ruledefs group_name
Assigns the specified group-of-ruledefs to this rulebase.
group_name must be the name of an existing group-of-ruledefs, and must be an alpha and/or numeric string of 1 through 63 characters in length.
When a group-of-ruledefs is specified, if any of the ruledefs within the group matches, the specified charging action is performed, any more of the action instances are not processed.

**Important:** If the group-of-ruledefs specified here is deleted or is not configured, the system accepts it without applying any ruledefs under current rulebase for this action priority.

charging-action charging_action_name
Specifies the charging action.
charging_action_name must be the name of an existing charging action, and must be an alpha and/or numeric string of 1 through 63 characters in length.
If the specified charging action does not exist, there will be no charging action triggers for this action priority within this rulebase.

**Important:** If the charging action specified here is deleted or not configured, the system accepts it without applying any charging action under current rulebase for this action priority.

monitoring-key monitoring_key
Associates the specified monitoring-key with ruledefs for usage monitoring.
monitoring_key must be an integer from 1 through 4000000000.
description description
Adds specified text to the rule and action.
description must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage
Use this command to configure action priorities for ruledefs / group-of-ruledefs in a rulebase.
This CLI command can be entered multiple times to specify multiple ruledefs and charging actions. The
ruledefs are examined in priority order, until a match is found and the corresponding charging action is
applied.

Example
The following command assigns a rule and action with the action priority of 23, a ruledef of test, and a charging
action of test1 to the current rulebase:
action priority 23 ruledef test charging-action test1
**bandwidth default-policy**

This command configures the default bandwidth policy for the current rulebase.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bandwidth default-policy policy
no bandwidth default-policy
```

no

Removes previously configured default bandwidth policy.

```
policy
```

Specifies the default bandwidth policy to be configured for the current rulebase. `policy` must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

Use this command to configure the default bandwidth policy for the current rulebase. This bandwidth policy will be used for subscribers using this rulebase for whom in the APN/Subscriber Configuration Mode the `default active-charging bandwidth-policy` command is configured, or no bandwidth policy is configured.

**Example**
The following command configures a bandwidth policy named `standard` for the rulebase:

```
bandwidth default-policy standard
```
billing-records

This command configures the type of billing to be performed for subscriber sessions.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
billing-records { egcdr | radius | rf | udr udr-format udr_format_name } +
no billing-records
```

- **egcdr**
  Generates an enhanced G-CDR (eG-CDR) and/or UDR with specified format on the occurrence of an interim trigger condition at the end of a subscriber session, or an SGSN-to-SGSN handoff.

- **radius**
  Generates postpaid RADIUS accounting records at the start and end of a subscriber session, and on the occurrence of an interim trigger condition. RADIUS accounting records are generated for each content ID.

  **Important:** In the GGSN, if in the APN configuration the “accounting-mode” is set to “none”, the system continues to send ACS-generated RADIUS accounting messages. In the PDSN, if in the subscriber default configuration the “accounting-mode” is set to “none”, the system does not send any RADIUS accounting messages (including ACS accounting messages).

- **rf**
  Enables Rf accounting.

- **udr udr-format udr_format_name**
  Generates UDRs with specified format on the occurrence of an interim trigger condition, at the end of a subscriber session or handoff.
  `udr_format_name` must be the name of an existing UDR format, and must be a string of 1 through 63 characters in length.

- **+**
  Indicates that more than one of the keywords can be entered in a single command.

Usage
Use this command to generate enhanced G-CDRs (eG-CDRs), RADIUS CDRs and/or UDRs for billing records. The format of eG-CDRs for the default GTPP group is controlled by the `Inspector` command in the Context Configuration Mode.

If, in the APN configuration, the “accounting-mode” is set as default (GTPP), and in the rulebase configuration “billing-records egcdr” is configured, both G-CDRs and eG-CDRs are generated if configured. If, in the APN, the accounting-mode is set to “none” G-CDRs will not be generated.

**Example**
The following command sets the billing record to UDR with UDR format named `udr_format1`:

```
billing-records udr udr-format udr_format1
```
cca diameter requested-service-unit

This command configures Diameter specific AVPs in Requested-Service-Unit group AVP with DCCA Credit Control Requests (CCRs).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
cca diameter requested-service-unit sub-avp { time cc-time duration | units cc-service-specific-units charging_unit | volume { cc-input-octets bytes | cc-output-octets bytes | cc-total-octets bytes } + }
```

```plaintext
no cca diameter requested-service-unit sub-avp
```

**no**
Disables the Diameter AVP configuration for DCCA CCRs.

```plaintext
time cc-time duration
```
Specifies requested service unit for charging time duration in seconds in included sub-AVP. 
**duration** specifies charging time in seconds and must be an integer from 1 through 4,294,967,295.

```plaintext
units cc-service-specific-units charging_unit
```
Specifies requested service unit by service specific units in bytes/packets in included sub-AVP. 
**charging_unit** specifies service-specific charging unit and must be an integer from 1 through 4,000,000,000.

```plaintext
volume { cc-input-octets bytes | cc-output-octets bytes | cc-total-octets bytes } +
```
Specifies requested service unit for charging octets by input, output and total volume in included sub-AVP. 
**cc-input-octets**: Specifies input charging octets. 
**cc-output-octets**: Specifies output charging octets. 
**cc-total-octets**: Specifies total charging octets. 
**bytes**: Specifies volume in bytes, and must be an integer from 1 to 4,000,000,000. 
**+**: More than one of the above keywords can be entered within a single command.

**Usage**
Use this command to include sub-AVPs based on time, volume, and service specific unit in Requested-Service-Unit group AVP with CCRs through Gy interface.

**Example**
The following command sets the time based sub-AVP with charging duration of 45 seconds in Requested-Service-Unit group AVP on DCCA CCRs:

```plaintext
```
cca diameter requested-service-unit sub-avp time cc-time 45
cca quota

This command is used to set various time and threshold-based quotas in the prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

{ no | default } cca quota { holding-time content-id cont_id | retry-time }

holding-time holding_time
Specifies the value for the Quota Holding Time (QHT). QHT is used with both time-based and volume-based quotas.
holding_time must be an integer from 1 to 4000000000.
After holding_time seconds has passed without user traffic, the quota is reported back and the charging stops until new traffic starts.

content-id cont_id
Specifies the content ID (Rating group AVP) to use for the Quota holding time for this rulebase.
cont_id is the specified content id for credit control service in an active charging service and must be an integer from 0 through 4,294,967,295.

retry-time retry_time [ max-retries retries ]
Default: 60
Specifies the retry time in seconds for the quota request.
retry_time must be an integer from 0 to 86400. To disable this assign 0.
This defines the maximum frequency at which the CC application tries to obtain quota for a subscriber passing traffic for a category with no/exhausted quota.
For a subscriber not passing traffic, the CC application will not try to obtain quota (except once at session start time, if so configured). i.e. the quota request from the no quota state is sent in response to user packets only, never based on a timer.
When subscriber hits a charging action that is a flow redirect, operator can optionally specify that this redirection shall clear the retry-time timer.
This allows the immediately following chargeable user traffic to trip a quota request, even if it would otherwise have been subject to the retry time limit. Such configuration allows quite large value for retry-time in quota charging or top up scenario.
max-retries retries option configures the maximum number of retries allowed for blacklisted categories. This option has default value of maximum retries of 65535 retries.
retries must be an integer from 1 through 65535. To disable this assign 0.

Usage
Use this command to set the prepaid credit control quotas.
cca quota retry time allows operator to set the amount of time that the ACS waits before it retries the prepaid server for a content id for which quota was exhausted earlier.
When server sends the quota holding time (QHT) it has highest priority to use that QHT irrespective of the value configured in rulebase or Credit Control Application configuration mode. QHT configured here has second priority for the content ID (rating group) configured here.

In case of QHT is not available from server and rulebase configuration mode, the QHT values configured at Credit Control Application configuration mode is used.

Example
The following command sets the prepaid credit control request retry time to 30 sec.:

```
cca quota retry-time 30
```

The following command sets the system to use the QHT from Credit Control Application mode:

```
no cca quota holding-time content-id content_id
```

The following command sets the system to ignore the QHT from Credit Control Application mode:

```
default cca quota holding-time content-id content_id
```

The following command sets the prepaid credit control request retry time to 60 seconds and maximum numbers of retries to 65535.

```
default cca quota retry-time max-retries
```
CCA QUOTA TIME-DURATION ALGORITHM

This command is used to define the algorithm used to compute time duration for prepaid credit control application quotas in the rulebase service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cca quota time-duration algorithm { consumed-time seconds | plus-idle | continuous-time-periods seconds | parking-meter seconds } [ content-id content_id ]
```

**Default cca quota time-duration algorithm**

```
cca quota time-duration algorithm { consumed-time | continuous-time-periods | parking-meter } [ content-id content_id ]
```

default

Sets the default configurations.

**consumed-time seconds**

Default: 0 (disabled)
Specifies the Quota Consumption Time (QCT) in seconds. QCT is used with active time-based quotas and to determine chargeable time envelopes for the purposes of consuming time quota.
Time envelope is the basis for reporting active usage. For each time envelope, the quota consumption includes the last QCT (duration between first packet and last packet + QCT).

**plus-idle**

Defines the idle time for QCT.
When used along with `consumed-time` it indicates the active usage + idle time, when no traffic flow occurs.

**continuous-time-periods seconds**

Default: 0 (disabled)
Specifies the charging quota continuous period in seconds.
The Continuous Time Periods (CTP) mechanism constructs a time-envelopes out of consecutive base time intervals in which traffic has occurred up to and including a base time interval which contains no traffic. As with Quota-Consumption-Time envelopes, the end of an envelope can only be determined “retrospectively”.
Again, as with Quota-Consumption-Time, the envelope for CTP includes the last base time interval, i.e. the one which contained no traffic.
seconds must be an integer from 1 through 4294967295.

**parking-meter** seconds

Default: 0 (disabled)

Specifies the Parking Meter (PM) period, in seconds, for particular rating group. This mechanism utilizes time quota, but instead of consuming linearly—once a decision to consume has been taken—the granted quota is consumed discretely in “chunks” of the base time interval at the start of each base time interval. Traffic is then allowed to flow for the period of the consumed quota. The time interval seconds defines the length of the Parking Meter. A time-envelope corresponds to exactly one PM (and thus to one base time interval). seconds must be an integer from 1 through 4294967295.

**content-id** content_id

Specifies the content ID (Rating group AVP) to use for the CCA Quota time duration algorithm selection in this rulebase. content_id is the specified content ID for credit control service in an active charging service, and must be an integer from 1 through 65535.

**session-time**

Specifies the session period in seconds. This is the default setting.

**Usage**

Use this command to set the various time charging algorithms/schemes for prepaid credit control charging. If operator chooses parking-meter seconds style charging, then time is billed in seconds chunks.

**Example**

The following command sets time duration to 400 seconds for prepaid credit control time duration algorithm:

```plaintext
cca quota time-duration algorithm consumed-time 400
```
cca radius accounting

This command specifies the accounting interval duration for RADIUS prepaid service parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] cca radius accounting interval interval
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes previously configured RADIUS accounting interval in the rulebase.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0 (Disabled).</td>
</tr>
<tr>
<td>Specifies the time interval, in seconds, between accounting actions.</td>
</tr>
<tr>
<td>interval must be an integer from 0 through 3600.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to specify the RADIUS accounting interval between accounting of a prepaid subscriber. The same parameters are applicable for RADIUS server group.

**Example**
The following command defines RADIUS accounting interval of 20 seconds for RADIUS prepaid service in a rulebase.
```
cca radius accounting interval 20
```
cca radius charging

This command specifies the charging context where RADIUS parameters are configured.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ no ] cca radius charging context vpn_context [ group group_name ]

no
Removes the previously configured RADIUS charging context in a rulebase.

context vpn_context
Specifies the charging context where RADIUS prepaid charging are configured.
vpn_context is an alpha and/or numeric string of 1 through 63 characters in length.

group group_name
Specifies the RADIUS server group name configured for RADIUS prepaid charging parameters.
group_name must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage
Use this command to specify the RADIUS charging context where RADIUS prepaid charging parameters are configured. The same parameters are applicable for RADIUS server group.

Example
The following command defines RADIUS charging context prepaid_rad1 for RADIUS prepaid charging in a rulebase:
cca radius charging context prepaid_rad1
cca radius user-password

This command specifies the RADIUS prepaid service subscriber’s user password parameters in a Rulebase.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] cca radius user-password [ encrypted ] password password
```

- **no**
  Removes the previously configured RADIUS prepaid service user password in a rulebase.

- **[ encrypted ] password password**
  Specifies the password to use for the user being given privileges for prepaid services within the current rulebase. The `encrypted` keyword indicates that the password specified uses encryption. `password` without encryption must be an alpha and/or numeric string of 1 through 63 characters, and when encrypted must be alpha and/or numeric string of 1 through 127 characters in length. The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**Usage**
Use this command to specify the RADIUS user password for prepaid services within the current rulebase.

**Example**
The following command defines the user password `user_123` without encryption for a prepaid service subscriber with RADIUS charging in a rulebase.

```
cca radius user-password password user_123
```
charging-rule-optimization

This command enables and sets the charging rule-optimization level for rule matching in a rulebase.

Product
All

Privilege
Security Administrator, Administrator

Syntax

charging-rule-optimization { high | low | medium }

default charging-rule-optimization

default
Sets the default charging rule search and matching optimization level.
Default: Low

high
Enables the highest efficient rule-searching organization with high memory utilization.

low
Enables minimally efficient rule-searching organization with minimal memory utilization.

medium
Enables moderately efficient rule-searching organization with medium memory utilization.

Usage
Use this command to specify the amount of internal optimization that is done for improved performance when evaluating each instance of the action CLI command.

Example
The following command specifies the highest optimization level for rule search and matching in a rulebase.

charging-rule-optimization high
constituent-policies

This command configures the bandwidth, CBB, and Firewall/Firewall-and-NAT constituent policies. The combination of the values of all three policies will uniquely identify a rulebase associated.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
constituent-policies { bandwidth-policy bandwidth_policy | cbb-policy cbb_policy | firewall-policy fw_policy | fw-and-nat-policy fw_nat_policy }+
```

**no constituent-policies**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the previous configuration.</td>
</tr>
</tbody>
</table>

**bandwidth-policy bandwidth_policy**

Specifies the Bandwidth policy.
`bandwidth_policy` specifies the bandwidth policy name, and must be a string of 1 through 63 characters in length.

**cbb-policy cbb_policy**

Specifies the CBB policy.
`cbb_policy` specifies the CBB policy name, and must be a string of 1 through 63 characters in length.

**firewall-policy fw_policy**

*Important:* This keyword is customer-specific.

Specifies the Firewall policy.
`fw_policy` specifies the Firewall policy name, and must be a string of 1 through 63 characters in length.

**fw-and-nat-policy fw_nat_policy**

*Important:* This keyword is customer specific, and is only available in StarOS 8.1.

Specifies the Firewall-and-NAT policy.
`fw_nat_policy` specifies the Firewall-and-NAT policy name, and must be a string of 1 through 63 characters in length.

**Usage**
Use this command to configure the bandwidth, CBB, and Firewall/Firewall-and-NAT constituent policies that will identify a rulebase. The combination of the values of all three policies will uniquely identify a rulebase associated.

Example
The following command configures the constituent Bandwidth policy named test123:

```
constituent-policies bandwidth-policy test123
```
content-filtering category policy-id

This command configures the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in a rulebase.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
content-filtering category policy-id cf_policy_id

no content-filtering category policy-id [ cf_policy_id ]
```

- **no**
  Removes the Content Filtering Category Policy configuration from the rulebase.
  In StarOS 8.1 and later, optionally the policy ID can be specified. If the specified policy ID is invalid, or is not configured in the rulebase, an error message is displayed. If no policy ID is specified, whatever policy is configured, if any, is removed from the rulebase.

```
category policy-id cf_policy_id
```

Configures the specified Content Filtering Category Policy in the current rulebase.

*cf_policy_id* must be the ID of an existing Content Filtering Category Policy, and must be an integer from 1 through 4294967295.

**Important:** In case the specified Content Filtering Category Policy does not exist, all packets will be passed regardless of the categories/actions determined for such packets.

**Important:** The category policy ID configured using the `category policy-id cf_policy_id` command in the APN/Subscriber Configuration mode prevails over this configuration.

**Usage**

Use this command to configure the Content Filtering Category Policy ID for Policy-based Content Filtering support in a rulebase.

The Content Filtering Category Policy is created/deleted in the Active Charging Service Configuration mode, and is configured in the Content Filtering Policy Configuration mode.

**Example**

The following command configures the policy ID 101 in the rulebase:

```
content-filtering category policy-id 101
```
content-filtering flow-any-error

This command configures allowing/discarding of Content Filtering packets in case of ACS error scenarios.

**Product**
ECS, CF

**Privilege**
Security Administrator, Administrator

**Syntax**

```
content-filtering flow-any-error { deny | permit }
default content-filtering flow-any-error
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the default setting.</td>
</tr>
<tr>
<td>Default: Permit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>deny</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures Content-Filtering flow-any-error as Deny.</td>
</tr>
<tr>
<td>All the denied packets will be accounted by “discarded-flow-content-id” configuration in the Content Filtering Policy ID Configuration Mode. I.e. this very content ID will be used to generate UDRs for the denied packets in case of Content Filtering.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>permit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures Content-Filtering flow-any-error as Permit.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to allow/discard content filtering packets in case of ACS error scenarios.

**Example**
The following command allows content filtering packets in case of ACS error:
```
content-filtering flow-any-error permit
```
content-filtering mode

This command enables the specified Content Filtering mode within a rulebase.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
content-filtering mode { category { static-only | static-and-dynamic } | server-group cf_server_group }
no content-filtering mode
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes/disables a previously configured content filtering mode in this rulebase.</td>
</tr>
<tr>
<td>It implies that content filtering in not to be performed for this rulebase.</td>
</tr>
<tr>
<td>This is the default mode.</td>
</tr>
</tbody>
</table>

| category { static-and-dynamic | static-only } |
|---|
| This keyword specifies the category-based content filtering mode. |
| **static-only** Configures Content Filtering mode as Static only. Compares all URLs against internal database to determine the category or categories of the requested content. |
| Use of this category-based content filtering support requires configuration of the require active-charging content-filtering category CLI command in the Global Configuration mode. |
| **static-and-dynamic** Configures Content Filtering mode as Static-and-Dynamic, wherein first static rating of the URL is performed, and only if the static rating fails to find a match dynamic rating of the content that the server returns is performed. |

**Important:** Before enabling static-and-dynamic rating in the rulebase, it must be enabled at the global level as the resources required for dynamic rating are allocated at the global level. To enable static-and-dynamic rating at the global level, in the Global Configuration Mode, use the require active-charging content-filtering category static-and-dynamic CLI command.

<table>
<thead>
<tr>
<th>server-group cf_server_group</th>
</tr>
</thead>
<tbody>
<tr>
<td>This keyword enables and configures the CFSG mode within a rulebase to manage an external content filtering server with an ICAP client system.</td>
</tr>
<tr>
<td>cf_server_group specifies the name of a pre-configured unique content filtering server group in Content Configuration Mode, and must be an alpha and/or numeric string of 1 through 63 characters in length.</td>
</tr>
<tr>
<td>If this keyword is used every ACS attempt to establish TCP connections to every server in the named group.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable and apply the content filtering mode within a rulebase to manage a content filtering server with an ICAP client system.
Example
The following command enables the content filtering mode for external content filtering server group \textit{CF\_Server1} with in this rulebase.

\texttt{content-filtering mode server-group CF\_Server1}

The following command enables the category based static and dynamic content filtering mode for with in this rulebase.

\texttt{content-filtering mode category static-and-dynamic}
**dynamic-rule**

This command configures the order of comparing the dynamic rules to static rules for the flow.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
dynamic-rule order { always-first | first-if-tied }
no dynamic-rule order

no

Removes the previously configured dynamic rule comparing order for this rulebase.

order { always-first | first-if-tied }

This command configures the way in which rules are selected for matching from dynamic rules list (per subscriber) and static rules list (from rulebase).

• **always-first**: If this option is configured, then all the dynamic rules are matched against the flow prior to any static rule.

• **first-if-tied**: If this option is configured, then rules are matched against the flow based on their priority with condition that dynamic rules match before a static rule of the same priority.

**Usage**

Use this command to configure the way in which rules are selected up for matching from dynamic rules list (per subscriber) and static rules list (from rulebase).

**Example**

The following command configures to match all dynamic rules against the flow prior to any static rule:

```plaintext
dynamic-rule order always-first
```
**edr suppress-zero-byte-records**

This command disables/enables the creation of EDRs when there is no data for the flows.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | default ] edr suppress-zero-byte-records
```

- **no**
  Disables the suppression of zero-byte EDRs.

- **default**
  Sets the default configuration.
  Default: `no edr suppress-zero-byte-records`

**Usage**

Use this command to disable/enable the creation of EDRs that are empty. The situation where there is a zero-byte EDR would typically be possible when two successive EDRs are generated for a flow. This CLI command suppresses the second such EDR for the flow.

**Example**

The following command disables the creation of zero-byte EDRs:

```
edr suppress-zero-byte-records
```
edr transaction-complete

This command configures the generation of an EDR on the completion of a transaction.

**Important**: This command is only available in StarOS 8.1 and StarOS 9.0 and later.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
edr transaction-complete http edr-format edr_format

{ default | no } edr transaction-complete
```

**default**
Sets the default configuration.
Default: same as `no edr transaction-complete`

**no**
Disables the generation of EDR on transaction completion.

**http**
Specifies EDR generation on transaction completion for HTTP protocol.

**edr-format edr_format**
Specifies the EDR format name.
`edr_format` must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**
Use this command to configure the generation of an EDR on the completion of a transaction. In this release EDR generation is supported only for HTTP protocol.

**Example**
The following command configures the generation of EDRs on the completion of transactions for HTTP protocol specifying the EDR format as `test123`:
```
edr transaction-complete http edr-format test123
```
**edr voip-call-end**

This command enables generating Event Data Record (EDR) on the completion of voice calls.

**Product**
ECS, P2P

**Privilege**
Security Administrator, Administrator

**Syntax**
```
edr voip-call-end edr-format edr_format_name
```

```
{ default | no } edr voip-call-end
```

- **default**
  Configures the default setting.
  Default: `no edr voip-call-end`

- **no**
  Specifies to disable EDR generation on the completion of a voice call.

- **edr-format edr_format_name**
  Specifies EDR format name.
  `edr_format_name` must be an existing EDR format’s name, and must be a string of 1 through 63 characters in length.

**Usage**
Use this command to enable generating EDR on the completion of voice calls. This facilitates P2P voice duration reporting.

**Example**
The following command specifies generating EDR on completion of voice calls using the EDR format `test13`:
```
edr voip-call-end edr-format test13
```
**egcdr inactivity-meter**

**Description** This command is obsolete. It is included in the CLI for backward compatibility with older configuration files. When executed performs no function. Use `egcdr threshold interval interval [ regardless-of-other-triggers ]` command for this functionality.
egcdr service-data-flow

This command assigns volume or interval threshold values to the interim Service Data Flow Containers in Flow Based Charging (FBC).

Product
GGSN, ECS

Privilege
Security Administrator, Administrator

Syntax

egcdr service-data-flow threshold { interval interval | volume { downlink | total | uplink } bytes }

{ no | default } egcdr service-data-flow threshold { interval | volume }

no
Removes the previously configured eG-CDR service data flow threshold for FBC.

default
Disables the egcdr service data flow threshold settings for FBC.

interval interval
Specifies the time interval (in seconds) for closing the eG-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow based charging. This option is disabled by default.
interval must be an integer from 60 through 400,000,000.

volume
Specifies the uplink/downlink volume octet counts for the generation of the interim eG-CDRs to service data flow container in FBC.

• downlink bytes - Sets the limit for the number of octets downlink after which the eG-CDR is closed. bytes (in bytes) must be an integer from 10,000 through 400000000. Default is 400,000,000.

• total bytes - Sets the limit for the total number of octets (uplink+downlink) after which the eG-CDR is closed. bytes (in bytes) must be an integer from 10,000 through 400,000,000. This configuration is disabled by default.

• uplink bytes - Sets the limit for the number of octets uplink after which the eG-CDR is closed. bytes (in bytes) must be an integer from 10,000 through 400,000,000. Default is 400,000,000.

Usage
Use this command to specify an eG-CDR threshold to generate it and write it to eG-CDR in service data flow container during flow based charging (FBC).

Example
The following command sets an eG-CDR threshold interval of \textbf{6000} seconds:

```
egcdr service-data-flow threshold interval interval 6000
```
egcdr tariff

This command sets the eG-CDR tariff time information to close and open new eG-CDR.

**Product**
GGSN, ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] egcdr tariff minute minute hour hour
```

- **no**
  - Removes the previously configured eG-CDR tariff.

- **minute minute**
  - Specifies the minute in a specified hour.
  - `minute` must be an integer from 0 through 59.

- **hour hour**
  - Specifies the hour of the day. `hour` must be an integer from 0 through 23.

**Usage**

Use this command to specify an eG-CDR tariff time. Up to 4 different time-of-day may be configured. When any tariff time reached the current eG-CDR will be closed and a new eG-CDR will be opened.

**Example**

The following command defines an eG-CDR tariff for the 23rd minute of the 22nd hour of the day:

```plaintext
egcdr tariff minute 23 hour 22
```
egcdr threshold

This command sets the eG-CDR volume or interval values to generate the interim eG-CDRs and write them to eG-CDR file.

Product
GGSN, ECS

Privilege
Security Administrator, Administrator

Syntax

```
egcdr threshold { interval interval [ regardless-of-other-triggers ] | volume { downlink | total | uplink } bytes }
{ no | default } egcdr threshold { interval | volume }
```

**no**
Removes previously configured eG-CDR threshold.

**default**
Disables the egcdr threshold settings.

**interval interval [ regardless-of-other-triggers ]**
Specifies the time interval (in seconds) for closing the eG-CDR if the minimum time duration thresholds are satisfied. This option is disabled by default. interval must be an integer from 60 to 4000000.

**regardless-of-other-triggers**: This option enables the eG-CDR generation at the fixed time interval irrespective of any other eG-CDR triggers that may have happened in between.

**volume**
Specifies the uplink/downlink volume octet counts for the generation of the interim eG-CDRs.

- **downlink bytes** - Sets the limit for the number of octets downlink after which the eG-CDR is closed. bytes (in bytes) must be an integer from 100,000 through 4,000,000,000. Default is 4,000,000,000.

- **total bytes** - Sets the limit for the total number of octets (uplink+downlink) after which the eG-CDR is closed. bytes (in bytes) must be an integer from 100,000 through 4,000,000,000. This configuration is disabled by default.

- **uplink bytes** - Sets the limit for the number of octets uplink after which the eG-CDR is closed. bytes (in bytes) must be an integer from 100,000 through 4,000,000,000. Default is 4,000,000,000.

Usage

Use this command to specify an eG-CDR threshold to generate it and write it to eG-CDR file.
Example
The following command defines an eG-CDR threshold interval of 600 seconds:

```
egcdr threshold interval 600
```
egcdr time-duration algorithm

This command is used to define the algorithm used to compute the duration for time utilization in eG-CDR for specific Rulebase.

Product
---
All

Privilege
---
Security Administrator, Administrator

Syntax
---

```plaintext
egcdr time-duration algorithm { consumed-time con_time [ plus-idle ] | continuous-time-periods ctp_seconds | parking-meter seconds }
{ default | no } egcdr time-duration algorithm

no
Removes the previously configured eG-CDR time-duration algorithm.

default
Sets default time duration value to time duration algorithm for eG-CDR generation.

consumed-time con_time [ plus-idle ]
Default: 0 (disabled)
Defines the actual consumption time in seconds. This is used to determine the actual used chargeable time envelopes for the purposes of consuming time quota.
Time envelope is the basis for reporting active usage. For each time envelope, the time consumption includes the time duration between arrival of last packet and first packet only.
con_time must be an integer from 1 through 4,294,967,295.
plus-idle: Defines the idle time between arrival of two packets to include in time usage record in eG-CDR.
When used along with consumed-time it indicates the active usage + idle time, when no traffic flow occurs.

continuous-time-periods ctp_time
Defines the continuous time period to compute the usage record in eG-CDR.
ctp_time sets the audition in seconds to start a counter on arrival of first packet and there after include only that period in charging in which one or more packets arrived. The period where no packets arrived or traffic detected no usage will be computed. ctp_time must be an integer from 1 through 4294967295.

parking-meter seconds
Defines the parking meter (PM) period in seconds.
Parking meter is the method with which the usage time is set in the content-id containers in eG-CDRs. When a parking meter value is set, the user is charged for time in increments of the value set. For example; if the parking meter value is set to 300 seconds (5 minutes) and the subscriber only uses one minute, the charge is for 5 minutes.
seconds must be an integer from 1 through 4294967295.
Usage
Use this command to set the various time charging algorithms/schemes for time usage in eG-CDR. For example, packets arrive at times T1, T2, T3 and T4. Then the typical time usage might be computed to be T4 – T1. However, if say there is an idle period between times T2 and T3, then system will compute the time usage to be (T2 – T1) + (T4 – T3).

consumed-time in above scenario calculates the time duration as (T2 – T1) + (T4 – T3) where consumed-time with plus-idle calculates the time duration as (T2-T1)+I + (T4 – T3)+I or (T4-T1).

Example
The following command sets consumed time duration to 400 seconds:

`egcdr time-duration algorithm consumed-time 400`
end

Returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to change to the Exec mode.
exit

Exits the Rulebase Configuration Mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to change to the parent configuration mode.
**extract-host-from-uri**

If the host field is not present in HTTP/WSP header, this command will extract host from URI, and store it in the host field.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
extract-host-from-uri { http | wsp } +
{ default | no } extract-host-from-uri
```

- **default**
  Configures the default setting.
  Default: `no extract-host-from-uri`

- **no**
  Removes the previous extract-host-from-uri configuration for all protocols.

- **http | wsp**
  Specifies protocol(s) for extract-host-from-uri configuration.

- **+**
  Indicates that more than one of the previous keywords can be entered within a single command.

**Usage**

If the host field is not present in HTTP/WSP header, this command will extract host from URI, and store it in the host field to enable “http host” and “wsp host” rule matches using the stored value.

**Important:** Applying the `extract-host-from-uri` command a second time will overwrite the previous configuration. For example, if you apply the command `extract-host-from-uri http wsp http` and then apply the command `extract-host-from-uri http wsp`, extraction of host from URI will happen only for WSP analyzer.

**Example**

The following command configures extraction of host from URI for both HTTP and WSP protocols:

```
extract-host-from-uri http wsp
```
**fair-usage**

This command configures a waiver on top of average available memory credits per session for the Fair Usage feature.

**Product**

ECS, CF, FW, NAT, P2P

**Privilege**

Security Administrator, Administrator

**Syntax**

```
fair-usage session-waiver-percent waiver_percent
default fair-usage session-waiver-percent
```

**default**

Configures the default setting.
Default: 20 percent

**session-waiver-percent waiver_percent**

Specifies the Fair Usage session waiver above average available memory for subscribers using the rulebase. `waiver_percent` must be an integer from 0 through 1000.

**Usage**

Use this command to configure a waiver on top of average available memory credits per session as a rulebase configuration.

**Example**

The following command configures the Fair Usage Session Waiver setting to 25 percent:

```
fair-usage session-waiver-percent 25
```
firewall dos-protection

This command configures protection for subscribers from Denial-of-Service (DoS) attacks.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce | ip-unaligned-timestamp | mime-flood | port-scan | tcp-window-containment | source-router | teardrop | winnuke }
```

**default firewall dos-protection**

no
Disables protection for subscribers from all or specified DoS attack(s).

**default**
Disables protection from all DOS attacks.

**all**
Enables protection against all DoS attacks supported by the Stateful Firewall service.

**flooding { icmp | tcp-syn | udp }**
Enables protection against specified flooding attack:
- **icmp:** Enables protection against ICMP Flood attack
- **tcp-syn:** Enables protection against TCP Syn Flood attack
- **udp:** Enables protection against UDP Flood attack

**ftp-bounce**
Enables protection against FTP Bounce attacks.
In an FTP Bounce attack, an attacker is able to use the PORT command to request access to ports indirectly through a user system as an agent for the request. This technique is used to port scan hosts discreetly, and to access specific ports that the attacker cannot access through a direct connection.

**ip-unaligned-timestamp**
Enables protection against IP Unaligned Timestamp attacks.
In an IP Unaligned Timestamp attack, certain operating systems crash if they receive a frame with the IP timestamp option that is not aligned on a 32-bit boundary.

**mime-flood**
Enables protection against HTTP Multiple Internet Mail Extension (MIME) header flooding attacks. In a MIME Flood attack an attacker sends huge amount of MIME headers which consumes a lot of memory and CPU usage.

**port-scan**
Enables protection against Port Scan attacks.

**tcp-window-containment**
Enables protection against TCP sequence number out-of-range attacks. In a Sequence Number Out of Range attack the attacker sends packets with out-of-range sequence numbers forcing the system to wait for missing sequence packets.

**source-router**
Enables protection against IP Source Route IP Option attacks. Source routing is an IP option mainly used by network administrators to check connectivity. When an IP packet leaves a system, its path through various networks to its destination is controlled by the routers and their current configuration. Source routing provides a means to override the control of the routers. Strict source routing specifies the path through all the routers to the destination. The same path in reverse is used to return responses. Loose source routing allows the attacker to spoof both an address and sets the loose source routing option to force the response to return to the attacker's network.

**teardrop**
Enables protection against Teardrop attacks. In a Teardrop attack, overlapping IP fragments are exploited causing the TCP/IP fragmentation re-assembly to improperly handle overlapping IP fragments.

**winnuke**
Enables protection against WIN-NUKE attacks. This is a type of Nuke denial-of-service attack against networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop. The WinNuke exploits the vulnerability in the NetBIOS handler and a string of out-of-band data sent to TCP port 139 of the victim machine causing it to lock up and display a Blue Screen of Death.

**Usage**
Use this command to enable firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

**Important:** The DoS attacks are detected only in the downlink direction.
The following command enables protection from all supported DoS attacks in the Inline Firewall Service:

```
firewall dos-protection all
```
firewall flooding

This command configures Firewall protection from Packet Flooding attacks.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit packets } | { sampling-interval interval } } 
```

```
default firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit } | { sampling-interval } }
```

```
default
Sets the specified firewall flooding configuration to the default value.
```

```
protocol { icmp | tcp-syn | udp }
```

Specifies the transport protocol:

- **icmp**: Configuration for ICMP protocol.
- **tcp-syn**: Configuration for TCP-SYN packet limit.
- **udp**: Configuration for UDP protocol.

```
packet limit packets
```

Specifies the maximum number of specified packets a subscriber can receive during a sampling interval. `packets` must be an integer from 1 through 4294967295. Default: 1000 packets per sampling interval for all protocols.

```
sampling-interval interval
```

Specifies the flooding sampling interval, in seconds. `interval` must be an integer from 1 through 60. Default: 1 second. The maximum sampling-interval configurable is 60 seconds.

**Usage**

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.
Example
The following command ensures a subscriber will not receive more than 1000 ICMP packets per sampling interval:

`firewall flooding protocol icmp packet limit 1000`

The following command ensures a subscriber will not receive more than 1000 UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IPs, those packets will be limited to 1000 packets per sampling interval. This way only “suspected” malicious packets are limited and not “legitimate” packets.

`firewall flooding protocol udp packet limit 1000`

The following command ensures a subscriber will not receive more than 1000 TCP-Syn packets per sampling interval.

`firewall flooding protocol tcp-syn packet limit 1000`

The following command specifies a flooding sampling interval of 1 second:

`firewall flooding sampling-interval 1`
firewall icmp-destination-unreachable-message-threshold

This command configures a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

default firewall icmp-destination-unreachable-message-threshold messages then-block-server

{ default | no } firewall icmp-destination-unreachable-message-threshold

- **default**
  Sets the default configuration.
  Default: No limit

- **no**
  Removes the previous configuration.

- **messages**
  Specifies the threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. `messages` must be an integer from 1 through 100.

**Usage**
Use this command to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked. Some servers that run QChat ignore the ICMP error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.

**Example**
The following command configures a threshold of 10 ICMP error messages:

```
firewall icmp-destination-unreachable-message-threshold 10 then-block-server
```
**firewall max-ip-packet-size**

This command configures the maximum IP packet size (after IP reassembly) allowed over firewall.

### Important:
In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall max-ip-packet-size packet_size protocol { icmp | non-icmp }

default firewall max-ip-packet-size protocol { icmp | non-icmp }
```

- **default**
  Sets the maximum IP packet size configuration to the default value.
  Default: 65535 bytes (for both ICMP and non-ICMP)

- **packet_size**
  Specifies the maximum packet size.
  `packet_size` must be an integer from 30000 through 65535.

- **protocol { icmp | non-icmp }**
  Specifies the transport protocol:
  - `icmp`: Configuration for ICMP protocol.
  - `non-icmp`: Configuration for protocols other than ICMP.

**Usage**

Use this command to configure the maximum IP packet size allowed for ICMP and non-ICMP packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for “Jolt Attack” and “Ping-Of-Death Attack”.

**Example**

The following command allows a maximum packet size of 60000 for ICMP protocol:

```plaintext
firewall max-ip-packet-size 60000 protocol icmp
```
firewall mime-flood

This command configures firewall protection from MIME Flood attacks.

**Important**: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product: FW
Privilege: Security Administrator, Administrator

Syntax:

```markdown
firewall mime-flood { http-headers-limit max_limit | max-http-header-field-size max_size }

default firewall mime-flood { http-headers-limit | max-http-header-field-size }
```

**default**

Sets the specified firewall MIME flood configuration to the default setting.

**http-headers-limit max_limit**

Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.

*max_limit* must be an integer from 1 through 256.

Default: 16

**max-http-header-field-size max_size**

Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.

*max_size* must be an integer from 1 through 8192.

Default: 4096 bytes

Usage:

Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks.

Example:

The following command sets the maximum number of headers allowed in an HTTP packet to 100:

`firewall mime-flood http-headers-limit 100`

The following command sets the maximum header field size allowed in the HTTP header to 1000 bytes:

`firewall mime-flood max-http-header-field-size 1000`
firewall mime-flood
**firewall no-ruledef-matches**

This command configures the default action for packets when no Firewall Ruledef matches.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, use the `access-rule no-ruledef-matches` command available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW, NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall no-ruledef-matches { downlink | uplink } action { deny [ charging-action charging_action ] | permit [ bypass-nat | nat-realm nat_realms ] }
```

```
default firewall no-ruledef-matches { downlink | uplink } action
```

- **default**
  Configures the default action for packets with no Firewall ruledef match.
  Default: uplink direction: permit, downlink direction: deny

- **downlink | uplink**
  Specifies the packet type:
  - **downlink**: Downlink packets with no Firewall ruledef match.
  - **uplink**: Uplink packets with no Firewall ruledef match.

- **action { deny [ charging-action charging_action ] | permit [ bypass-nat | nat-realm nat_realms ] }**
  Specifies the default action for packets with no Firewall ruledef match.
  - **permit [ bypass-nat | nat-realm nat_realms ]**: Permit packets. Optionally specify:
    - **bypass-nat**: The `bypass-nat` keyword is only available in StarOS 8.3 and later.
    - **nat-realm**: Specifies to bypass Network Address Translation (NAT).
    - **nat-realm nat_realms**: Specifies a NAT realm to be used for performing NAT on subscriber packets. `nat_realms` must be an alpha and/or numeric string of 1 through 31 characters in length.

**Important:** If neither `bypass-nat` or `nat-realm` are configured, NAT is performed if the `nat policy nat-required` CLI command is configured with the `default-nat-required` option.

- **deny [ charging-action charging_action ]**: Deny specified packets.
Optionally, a charging action can be specified. `charging_action` must be the name of a charging action, and must be a string of 1 through 63 characters in length.

**Usage**

Use this command to configure the default action to be taken on packets with no Firewall ruledef matches. If, for deny action, the optional charging action is configured, the action taken depends on what is configured in the charging action. For the firewall rule, the “flow action”, “billing action”, and “content ID” of the charging action will be used to take action. If flow exists, flow statistics are updated. Allowing/dropping of packets is determined in the following sequence:

- **Check** is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
- Firewall ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the `firewall priority` configuration.
- If no firewall ruledef matches, the packet is allowed or dropped as per the `no-ruledef-matches` configuration.

For a packet dropped due to firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the `firewall priority` or the `firewall no-ruledef-matches` command respectively.

In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the `access-rule priority` or the `access-rule no-ruledef-matches` command respectively. For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the `flow any-error charging-action` command.

**Example**

The following command sets Firewall to permit downlink packets with no ruledef matches:

```
firewall no-ruledef-matches downlink action permit
```
**firewall policy**

This command enables/disables Stateful Firewall support for all subscribers using this rulebase.

### Important:
In StarOS 8.0, this command is available in the APN/Subscriber Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall policy firewall-required
{ default | no } firewall policy
```

- `default`:
  Sets the default firewall support setting for all subscribers using this rulebase.
  Default: Disabled

- `no`:
  Disables firewall support for all subscribers using this rulebase.

- `firewall-required`:
  Enables firewall support for all subscribers using this rulebase.

**Usage**

Use this command to enable/disable firewall support for all subscribers using this rulebase.

**Example**
The following command enables Stateful Firewall support:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support:

```
no firewall policy
```
**firewall priority**

This command adds and specifies the priority and type of a firewall ruledef in the rulebase, and allows to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

**Important:** In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, use the `access-rule priority` command available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW, NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall priority priority [ dynamic-only | static-and-dynamic ] firewall-ruledef firewall-ruledef { { deny [ charging-action charging_action ] } | { permit [ nat-realm nat_realm | [ trigger open-port { aux_port_number | range start_port_number to end_port_number } direction { both | reverse | same } ] ] } }

no firewall priority priority
```

- **no**
  Removes the previously configured firewall ruledef priority from the rulebase.

- **priority**
  Specifies the firewall ruledef’s priority in the rulebase.
  `priority` must be unique, and must be an integer from 1 through 65535.

- **[ dynamic-only | static-and-dynamic ] firewall-ruledef firewall-ruledef**
  Specifies the firewall ruledef to add to the rulebase. Optionally, the firewall ruledef type can be specified.

  - **dynamic-only**: Firewall Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.
  - **static-and-dynamic**: Firewall Static and Dynamic Ruledef—Predefined ruledef that can be disabled/enabled by the policy server, and is enabled by default.

  `firewall-ruledef` must be the name of a predefined firewall ruledef, and must be a string of 1 through 63 characters in length.

- **deny [ charging-action charging_action ]**
  Denies packets if the rule is matched. An optional charging action can be specified. If a packet matches the deny rule, action is taken as configured in the charging action. For firewall ruledefs, only the terminate-flow action is applicable, if configured in the specified charging action.

  `charging_action` must be a string of 1 through 63 characters in length.
permit [ nat-realm nat-realm ] [ bypass-nat ] [ trigger open-port { aux_port_number | range start_port_number to end_port_number } ] ]

Permits packets.

nat-realm: Specifies the NAT realm to be used for performing NAT on subscriber packets matching the firewall ruledef.

If the NAT realm is not specified, then NAT will be bypassed. That is, NAT will not be applied on subscriber packets that are matching a firewall ruledef with no NAT realm name configured.

nat-realm specifies the NAT realm name, and must be a string of 1 through 31 characters in length.

bypass-nat: Specifies that packets bypass Network Address Translation (NAT).

**Important:** If the nat-realm is not configured, NAT is performed if the nat policy nat-required CLI command is configured with the default-nat-realm option.

trigger open-port { aux_port_number | range start_port_number to end_port_number}: Permits packets if the rule is matched, and allows the creation of data flows for firewall. Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.

aux_port_number: Specifies the number of auxiliary ports to open for traffic, and must be an integer from 1 through 65535.

range start_port_number to end_port_number: Specifies the range of ports to open for subscriber traffic.

start_port_number must be an integer from 1 through 65535. This is the start of the port range and must be less than end_port_number.

end_port_number must be an integer from 1 through 65535. This is the end of the port range and must be greater than start_port_number.

direction { both | reverse | same }:

Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.

both: Provides the trigger to open port for traffic in either direction of the control connection.

reverse: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).

same: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).

Usage

Use this command to add firewall ruledefs to the rulebase and configure the priority, type, and port triggers. Port trigger configuration is optional. Port trigger can be configured only if a rule action is permit.

The rulebase specifies the firewall rules to be applied on the calls. The ruledefs within a rulebase have priorities, based on which priority matching is done. Once a rule is matched and the rule action is permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association which matches the rule.

Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic.

Once a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, EDR is generated.
If the content ID is configured, UDR information is updated.

If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

**Important:** For firewall ruledefs, only the terminate-flow action is applicable if configured in the specified charging action.

For a packet dropped due to firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the `firewall priority` or the `firewall no-ruledef-matches` command respectively.

In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the `access-rule priority` or the `access-rule no-ruledef-matches` command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the `flow any-error charging-action` command.

The GGSN can dynamically activate/deactivate dynamic firewall ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the rulebase is a dynamic rule, and if the rule is enabled for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

**Example**

The following command assigns a priority of 10 to the firewall ruledef `fw_rule1`, adds it to the rulebase, and permits port trigger to be used for the rule to open ports in the range of 100 to 200 in either direction of the control connection:

```
firewall priority 10 firewall-ruledef fw_rule1 permit trigger open-port range 100 to 200 direction both
```

The following command configures the firewall ruledef `fw_rule2` as a dynamic ruledef:

```
firewall priority 7 dynamic-only firewall-ruledef fw_rule2 deny
```
firewall tcp-first-packet-non-syn

This command configures the action to take on TCP flow starting with a non-syn packet.

---

**Important:** In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

---

**Product**

FW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
firewall tcp-first-packet-non-syn { drop | reset }
```

```
default firewall tcp-first-packet-non-syn
```

- **default**
  - Sets the default action setting.
  - Default: drop

- **drop | reset**
  - Specifies the action to take on TCP flow starting with a non-syn packet.
  - **drop**: Drops the packet or session
  - **reset**: Sends reset

**Usage**

Use this command to configure action to take on TCP flow starting with a non-syn packet.

**Example**

The following command configures action to take on TCP flow starting with a non-syn packet to drop:

```
firewall tcp-first-packet-non-syn drop
```
firewall tcp-idle-timeout-action

This command configures action to take on TCP idle timeout expiry.

**Important:** In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
firewall tcp-idle-timeout-action { drop | reset }
```

```
default firewall tcp-idle-timeout-action
```

default
Sets the default action setting.
Default: reset

drop | reset
Specifies the action to take on TCP timeout expiry.
drop: Drops the packet or session
reset: Sends reset

**Usage**
Use this command to configure action to take on TCP idle timeout expiry.

**Example**
The following command configures action to take on TCP idle timeout expiry to drop:

```
firewall tcp-idle-timeout-action drop
```
firewall tcp-reset-message-threshold

This command configures a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

**Important:** This command is only available in StarOS 8.3 and later. In StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

`firewall tcp-reset-message-threshold messages then-block-server`

{ default | no } `firewall tcp-reset-message-threshold`

**default**

Configures the default setting.
Default: The same as `no firewall tcp-reset-message-threshold`

**no**

Removes the previous configuration.

**messages**

Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. `messages` must be an integer from 1 through 100.

**Usage**

Use this command to configure a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked. This configuration enables QCHAT noise suppression for TCP.

**Example**

The following command sets the threshold on the number of TCP reset messages to 10:

`firewall tcp-reset-message-threshold 10 then-block-server`
firewall tcp-syn-flood-intercept

This command enables and configures the TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the dos-protection command.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
firewall tcp-syn-flood-intercept { mode { none | watch [ aggressive ] } } | watch-timeout intercept_watch_timeout

default firewall tcp-syn-flood-intercept { mode | watch-timeout }

default

Sets the default values of TCP intercept parameters for SYN Flood DoS protection.
```

```plaintext
mode { none | watch [ aggressive ] }

Specifies the TCP SYN flood intercept mode:
- **none:** Disables TCP SYN flood intercept feature.
- **watch:** Configures TCP SYN flood intercept feature in watch mode. The firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, the firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive:** Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

Default: **none**
```

```plaintext
watch-timeout intercept_watch_timeout

Specifies the TCP intercept watch timeout, in seconds.
```

**Default:**

- `intercept_watch_timeout` must be an integer from 5 through 30.
- Default: 30
Usage
This TCP intercept functionality provides protection against TCP SYN Flooding attacks. The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

Example
The following command sets the TCP intercept watch timeout setting to 5 seconds:
firewall tcp-syn-flood-intercept watch-timeout 5
**flow any-error**

This command specifies the charging action to be used for packets dropped by Firewall due to any error conditions.

**Product**
FW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
flow any-error charging-action charging_action
default flow any-error
```

**default**

Configures the default action for packets dropped by Firewall due to any errors.
Default: Update the flow stats if flow is available

**charging-action charging_action**

Specifies the charging action based on which accounting action is taken on packets dropped by Firewall due to any errors.

**Important:** The charging action specified here should preferably not be used for action on packets dropped due to firewall ruledef match or no-match (in the `firewall priority` and `firewall no-ruledef-matches` commands) and the content ID within the charging action must be unique so that dropped counts will not interfere with other content IDs.

**charging_action** must be the name of a charging action, and must be a string of 1 through 63 characters in length.

**Usage**

Use this command to configure the charging action for packets dropped by Firewall due to any error conditions, such as, a packet being inappropriate based on the state of the protocol of the packet's session, or Firewall DoS protection causing the packet to be discarded, and so on.
For a packet dropped due to firewall ruledef match or no-match (first packet of a flow), the charging action applied is the one configured in the `firewall priority` or the `firewall no-ruledef-matches` command respectively.
In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the `access-rule priority` or the `access-rule no-ruledef-matches` command respectively.
For a packet dropped due to any error condition after data session is created, the charging action used is the one configured in the `flow any-error charging-action` command.
If the charging action applied on a packet is the one specified in the `flow any-error charging-action` command, flow statistics are updated and action is taken as configured in the charging action:
- If the billing action is configured as EDR enabled, EDR is generated.
- If the content ID is configured, UDR information is updated.
If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

Example
The following command specifies the charging action test2 for accounting action on packets dropped/discarded by Firewall due to any error:

```
flow any-error charging-action test2
```
flow control-handshaking

This command specifies how to charge for the control traffic associated with an application.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
flow control-handshaking { charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-packets ] } | charge-separate-from-application }

default flow control-handshaking

no flow control-handshaking [ charge-to-application ]
```

```
no flow control-handshaking [ charge-to-application ]

Removes the previous flow control-handshaking configuration. The control packets will use whatever
content-id is determined by the normal use of the action CLI commands.
In this command, the optional keyword charge-to-application is deprecated and has no effect.

default flow control-handshaking

Configures the default setting.
Default: The same as no flow control-handshaking.

charge-to-application

This keyword configures the charging action to include the flow control packets either during initial
handshaking only or specified control packets during session for charging.

all-packets

Specifies that the initial setup packets will wait until the application has been determined before assigning the
content-id, and all mid-session ACK packets, as well as, the final tear-down packets will use that content-id.

initial-packets

Specifies that only the initial setup packets will wait for content-id assignment.

mid-session-packets

Specifies that the ACK packets after the initial setup will use the application's or content-id assignment.

tear-down-packets

Specifies that the final tear-down packets (TCP or WAP) will use the application's or content-id assignment.
charge-separate-from-application

This keyword configures the charging action to separate the charging of the initial control packets or all subsequent control packets from regular charging.

Usage

Use this command to configure how to charge for the control traffic associated with an application ruledef. Applications like HTTP use TCP to set up and tear down connections before the HTTP application starts. This CLI command controls whether the packets that set up and tear down the connections should use the same content ID as the application’s flow.

In normal mode 3-way handshake TCP packets (SYN, SYN-ACK, and ACK) and closing or intermittent packets (FIN, RST, etc.) directed and charged based on configured matched rules. This command makes the system to wait for the start and stop of layer 7 packet flow and content ID and charge the initial, intermittent, and closing TCP packets as configured to the same matching rules and content ID as of the flow.

This CLI command also affects applications that do not use TCP but use other methods for control packets, e.g., WAP where WTP/UDP may be used to set up and tear down connection-oriented WSP.

Example

Following command enables the charging for initial TCP handshaking control packets and wait for content-id of data traffic flow:

```
flow control-handshaking charge-to-application initial-packets
```

The following command enables charging all mid-session ACKs as well as tear-down packets to application:

```
flow control-handshaking charge-to-application mid-session-packets tear-down-packets
```
flow end-condition

This command sets the end condition of the session flows related to a user session and triggers the EDR generation.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
flow end-condition { { content-filtering | normal-end-signaling | timeout + } | { { hagr | handoff | session-end } [ flow-overflow ] + } [ url-blacklisting ] }
edr edr_format

no flow end-condition
```

**no**
Removes the previously configured end condition of the EDR flow related to a user session.

**content-filtering**
Specifies to create an EDR with format named `edr_format` when category-based content filtering application action leads to a flow end. Possible Content-filtering actions redirect-url, terminate-flow, content-insert.

**hagr**
Specify to create an EDR with format named `edr_format` when flow ended due to session handoff according to Interchassis Session Recovery support.

**handoff**
Specify to create an EDR with format named `edr_format` when flow ended due to hand-off. Whenever a handoff occurs, ACS closes the EDRs for all current flows using the EDR format `edr_format`, and begin new statistics collection for the flows for the EDRs that will be generated when the flows actually end.

**normal-end-signaling**
Specifies the flow end condition as normal when a flow end is signaled normally like detecting FIN and ACK for a TCP flow, or a WSP-DISCONNECT terminating a connection-oriented WSP flow over UDP) and create an EDR for the flow using the EDR format `edr_format`.

**session-end**
Specify to create an EDR when a subscriber session ends. By this option ACS creates an EDR with format named `edr_format` for every flow that has had any activity since last EDR was created for the flow on session end.

**timeout**
Specify to create an EDT with format named `edr_format` when a flow ends or deleted due to a timeout condition.
flow end-condition

flow-overflow

**Important:** This keyword is only available in StarOS 8.3 and later. And, is only applicable when used with the `hagr`, `handoff`, and `session-end` keywords.

Specifies generation of flow-overflow EDR for conditions that affect the callline. If any of the specified end-conditions that affect subscriber information stored at ACS (i.e. callline) is configured the “flow-overflow” EDR is generated.

url-blacklisting

Specifies to create an EDR with format named `edr_format` when URL Blacklisting application action leads to a flow end.

+ More than one of the keywords can be entered within a single command.

edr `edr_format`

Specifies the EDR format name to record EDR in specified flow end condition. `edr_format` is a pre-configured format, and must be a unique alpha and/or numeric string 1 through 63 characters in length.

**Usage**

Use this command to enable or disable the capturing of EDRs based on flow end condition.

**Example**

The following command defines the end condition as handoff for flow and creates an EDR with as per format named `EDR_format1`:

```
flow end-condition handoff edr-format EDR_format1
```
flow limit-across-applications

This command limits the total number of simultaneous flows per Subscriber/APN sent to a rulebase regardless of the flow type, or limit flows based on the protocol type under the Session Control feature.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
flow limit-across-applications { limit | non-tcp limit | tcp limit }
```

```
no flow limit-across-applications [ non-tcp | tcp ]
```

- **no**
  - Removes previously configured flow limit related to a rulebase.

- **limit**
  - Specifies the maximum number of flows across all applications for a rulebase.
  - `limit` must be an integer from 1 through 4000000000.
  - Default: No limits

- **non-tcp limit**
  - Specifies the maximum limit of non-TCP type flows.
  - `limit` must be an integer from 1 through 4000000000.
  - Default: No limits

- **tcp limit**
  - Specifies the maximum limit of TCP flows.
  - `limit` must be an integer from 1 through 4000000000.
  - Default: No limits

Usage

Use this command to limit the total number of flows allowed for a rulebase regardless of flow type, or limit flows based on the protocol—non-TCP (connection-less) or TCP (connection-oriented).

If a subscriber attempts to exceed these limits system discards the packets of new flow. This limit processing of this command has following aspects for UDP, TCP, ICMP and some of the exempted flows:

UDP/ICMP: System waits for the flow timeout before updating the counter and removing it from the count of number of flows.

TCP: After a TCP flow ends, system waits for a short period of time to accommodate the retransmission of any missed packet from one end. TCP flows those are ended, but are still in wait period for timeout are exempted for this limit processing.

Exempted flows: System exempts all the other flows specified with the `flow limit-for-flow-type` command in the Charging Action Configuration Mode set to no.
Example
The following command defines the maximum number of 200000 flows for a rulebase:

```
flow limit-across-applications 200000
```
fw-and-nat default-policy

This command configures the default Firewall-and-NAT policy for an ACS Rulebase.

**Important:** This command is only available in StarOS 8.1 and StarOS 9.0 and later. This command must be used to configure the Policy-based Firewall-and-NAT feature.

**Product**
- FW, NAT

**Privilege**
- Security Administrator, Administrator

**Syntax**

```
fw-and-nat default-policy fw_nat_policy
no fw-and-nat default-policy
```

**Usage**
Use this command to configure the default Firewall-and-NAT policy for an ACS rulebase. This policy is used for a subscriber only if:
- In the APN/subscriber configuration modes, the `default fw-and-nat policy` command is configured.
- Or, a policy to use is not received from the AAA/OCS.

For more information, see the *Personal Stateful Firewall Administration Guide*.

**Example**
The following command configures a Firewall-and-NAT policy named `standard` to the rulebase:

```
fw-and-nat default-policy standard
```
ip reassembly-timeout

This command configures how long to hold onto IP fragments for reassembly, while waiting for the complete packet to arrive.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ip reassembly-timeout timeout_duration

default ip reassembly-timeout
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the timeout timer to 5000 milliseconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>timeout_duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the user configured value to timeout timer to hold fragmented packets before reassembly.</td>
</tr>
<tr>
<td><code>timeout_duration</code> is the duration, in milliseconds, and must be an integer from 100 through 30000.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure duration for timeout timer to hold IP fragmented packets before reassembly is needed.

IP fragmented packet are retained, until either all fragmented packets have been received or the configured timeout has expired for the oldest fragment. If all fragments have been received, a temporary complete packet is reconstructed for analysis. Then all fragments are forwarded in order from first to last. If all fragments are not received, the fragments will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.

**Example**

The following command sets the timeout timer to 15000 milliseconds:

```plaintext
ip reassembly-timeout 15000
```
ip reset-tos

This command enables the system to reset the IP Type of Service (ToS) value to zero.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ default | no ] ip tos-reset

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the default configuration.</td>
</tr>
<tr>
<td>Default: Do not reset the ToS to zero</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the previous configuration.</td>
</tr>
</tbody>
</table>

Usage

Use this command to reset the ToS field of any packet after it reaches ECS, or to broaden the range of values that are used in the ToS field in the IP header of any packet.
**nat binding-record**

Configures the NAT binding record generation setting.

**Important:** This command is only available in StarOS 8.3. In StarOS 9.0 this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Syntax**

```
nat binding-record edr-format edr_format [ port-chunk-allocation ] [ port-chunk-release ] +
{ default | no } nat binding-record
```

- **default**
  
  Configures the default setting.
  
  Default: port-chunk-release

- **no**
  
  Deletes the previous NAT binding record configuration.

- **edr-format edr_format**
  
  Specifies the EDR format name.
  
  edr_format must be an alpha and/or numeric string of 1 through 63 characters in length.

- **port-chunk-allocation**
  
  Specifies generating NAT bind record when a port chunk is allocated.

- **port-chunk-release**
  
  Specifies generating NAT bind record when a port chunk is released.

- **+**
  
  Indicates that more than one of the previous keywords can be entered within a single command.

**Usage**

Use this command to configure the NAT binding record generation setting.

**Example**
The following command configures an EDR format named `test123` and specifies generating NAT binding record when a port chunk is allocated, and when a port chunk is released:

```
nat binding-record edr-format test123 port-chunk-allocation port-chunk-release
```
**nat policy**

This command enables/disables Network Address Translation (NAT) processing for all subscribers using this rulebase.

**Important:** In StarOS 8.1 and StarOS 9.0 and later, for Policy-based Firewall-and-NAT, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Important:** Before enabling NAT processing for a subscriber, Firewall must be enabled for the subscriber. See the `firewall policy` CLI command.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nat policy nat-required [ default-nat-realm realm_name ]
{ default | no } nat policy
```

- **default**
  Sets the default NAT processing setting for all subscribers using this rulebase.
  Default: Disabled

- **no**
  Disables NAT processing for all subscribers using this rulebase.

- **nat-required**
  Enables NAT processing for all subscribers using this rulebase.

```
default-nat-realm realm_name
```

**Important:** This keyword is only available in StarOS 8.3 and later.

Specifies the default NAT realm to be used if one is not already configured.

*realm_name* must be an alpha and/or numeric string of 1 through 31 characters in length.

**Important:** Including the default NAT realm, a maximum of three NAT realms are supported.

**Usage**

Use this command to enable/disable NAT processing for all subscribers using this rulebase.
Once NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms defined in the rule priority lines within the rulebase. See the `firewall priority` CLI command.
NAT enable/disable status in the rulebase can be changed any time, however the changed NAT status will not be applied for active calls using the rulebase. The new NAT status is only applied to new calls.

**Example**
The following command enables NAT processing:

```
nat policy nat-required
```

The following command disables NAT processing:

```
no nat policy
```
nat suppress-aaa-update

This command suppresses the sending of NAT bind updates (NBU) to the AAA server when PPP disconnect happens.

**Important:** This command is customer-specific. For more information please contact your local service representative. In StarOS 9.0, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
nat suppress-aaa-update call-termination

default nat suppress-aaa-update
```

**Usage**

Use this command to suppress the sending of NAT bind updates (NBU) to the AAA server when PPP disconnect happens, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NAT bind updates are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

**Example**

The following command suppresses the sending of NAT bind updates (NBU) to the AAA server when PPP disconnect happens:

```bash
nat suppress-aaa-update call-termination
```
**p2p dynamic-flow-detection**

This command enables the P2P analyzer to detect P2P applications configured for the Active Charging service.

**Product**

P2P

**Privilege**

Security Administrator, Administrator

**Syntax**

```
p2p dynamic-flow-detection
{ default | no } p2p dynamic-flow-detection
```

- **default**
  Configures the default setting.
  Default: `no p2p dynamic-flow-detection`

- **no**
  Disables detecting P2P applications with the P2P analyzer.

**Usage**

Use this command to set up dynamic-flow detection. This allows the P2P analyzer to detect the P2P applications configured for the Active Charging service.
post-processing priority

This command configures the post-processing priority and action to be taken on the specified ruledef in the rulebase.

**Important:** This command is only available in StarOS 8.3 and later.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
post-processing priority priority { group-of-ruledefs group_name | ruledef ruledef_name } charging-action charging_action_name [ description description ]
```

```
no post-processing priority priority
```

```
priority priority
```
Specifies priority for the ruledef/group-of-ruledefs in the rulebase.

*priority* must be an integer from 1 through 65535, and must be unique.

```
group-of-ruledefs group_name
```
Assigns the specified group-of-ruledefs to the rulebase.

*group_name* must be the name of a group-of-ruledefs, and must be an alpha and/or numeric string of 1 through 63 characters in length.

**Important:** The group-of-ruledefs specified must be configured for post-processing. See the **group-of-ruledefs-application** CLI command in the Group-of-Ruledefs Configuration mode.

```
ruledef ruledef_name
```
Assign the specified ruledef to the rulebase.

*ruledef_name* must be an alpha and/or numeric string of 1 through 63 characters in length.

**Important:** The ruledef specified must be configured for post-processing. See the **rule-application** CLI command in the Ruledef Configuration mode.

```
charging-action charging_action_name
```
Specifies the charging action.

*charging_action_name* must be an alpha and/or numeric string of 1 through 63 characters in length.

```
description description
```
Specifies optional description for this configuration.

*description* must be an alpha and/or numeric string of 1 through 31 characters in length.
Usage

Use this command to configure the post-processing priority and action to be taken on a ruledef in the rulebase.

Example

The following command configures the ruledef named `test_ruledef` with a priority of 10, and the charging action named `test_ca` for post processing:

```
post-processing priority 10 ruledef test_ruledef charging-action test_ca
```
post-processing dynamic

This command configures specified ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs enabling to differentiate between normal post-processing rules from pre-configured ones. Default: Disabled

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

post-processing dynamic { group-of-ruledefs group_name | ruledef ruledef_name }
charging-action charging_action [ description description ]

no post-processing dynamic { group-of-ruledefs group_name | ruledef ruledef_name }

no
Removes the specified post-processing dynamic configuration.

group-of-ruledefs group_name
Assigns the specified group-of-ruledefs to the current rulebase.
group_name must be an alpha and/or numeric string of 1 through 63 characters in length.

ruledef ruledef_name
Assigns the specified ruledef to the current rulebase.
ruledef_name must be an alpha and/or numeric string of 1 through 63 characters in length.

charging-action charging_action
Specifies charging action.
charging_action must be an alpha and/or numeric string of 1 through 63 characters in length.

description description
Specifies optional description for this configuration.
description must be an alpha and/or numeric string of 1 through 31 characters in length.

Usage
Use this command to configure specific ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs enabling to differentiate between normal post-processing rules from the pre-configured ones. This makes possible enabling/disabling ruledefs/groups-of-ruledefs entry from external server.

Example
post-processing dynamic

The following command specifies the ruledef named `test_rule` as a dynamic post-processing ruledef configured with the charging action `ca13` and a description of `testing`:

```
post-processing dynamic ruledef test_rule charging-action ca13 description testing
```
qos-renegotiate timeout

This command configures the timeout setting for the Quality of Service (QoS) Renegotiation feature.

**Important:** This command is controlled by the dynamic-qos-renegotiation license.

### Product
All

### Privilege
Security Administrator, Administrator

### Syntax

```plaintext
qos-renegotiate timeout timeout
no qos-renegotiate timeout

no
Disables timeout setting if previously configured.

timeout timeout
Specifies the timeout period for QoS Renegotiation feature in this rulebase.
`timeout` must be the timeout period, in seconds, and must be an integer from 0 through 4294967295.
If set to 0, timeout is disabled.
```

### Usage

Use this command to configure timeout setting for the QoS Renegotiation feature.

### Example

The following command sets the QoS renegotiate timeout period to 1000 seconds:

```
qos-renegotiate timeout 1000
```
radius threshold

This command sets the interval and volume thresholds to generate the interim RADIUS CDRs and write them to CDR file for ECS postpaid billing.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
radius threshold { interval interval | volume total volume }
{ no | default } radius threshold { interval | volume total }
```

- **no**
  Removes the previously RADIUS threshold configuration.

- **default**
  Configures the default settings.

- **interval interval**
  Default: Disabled
  Specifies the time interval (in seconds) for generating RADIUS interim accounting requests. This option is disabled by default. **interval** must be an integer from 60 through 40000000.

- **volume total volume**
  Default: Disabled
  Specifies the limit for the total number of octets (uplink+downlink) after which a stop-start pair will be sent to RADIUS. **volume** must be an integer from 100,000 to 4,000,000,000.

**Usage**

Use this command to specify a time interval threshold to generate interim RADIUS CDRs and write it to RADIUS CDR file for postpaid billing.

**Example**
The following command defines a time threshold interval of 600 seconds for RADIUS CDRs:

```
radius threshold interval 600
```
route priority

This command controls routing of packets to protocol analyzers.

Product
All

Privilege
Security Administrator, Administrator

Syntax


no route priority route_priority

no
Removes the specified route configuration from the current rulebase.

priority route_priority

Specifies the route priority for the ruledef in the current rulebase.
route_priority must be an integer from 1 through 65535.
Lower numbered priorities are examined first. Up to 1024 instances can be configured across all rulebases.

ruledef ruledef_name

Specifies the ruledef to evaluate packets to determine the analyzer.
ruledef_name specifies the name of an existing ruledef configured for the route application using the rule-application command in the Ruledef Configuration Mode.

analyzer

Specifies the analyzer for the ruledef, and must be one of the following:
  • dns: Route to DNS protocol analyzer.
  • file-transfer: Route to file analyzer.
  • ftp-control: Route to FTP control protocol analyzer.
  • ftp-data: Route to FTP data protocol analyzer.
  • http: Route to HTTP protocol analyzer.
  • imap: Route to IMAP protocol analyzer.
  • mms: Route to MMS protocol analyzer.
  • p2p: Route to the P2P protocol analyzer.
  • pop3: Route to POP3 protocol analyzer.
  • pptp: Route to PPTP protocol analyzer.
  • rtcp: Route to RTCP protocol analyzer.
- \textbf{rtp}: Route to RTP protocol analyzer.
- \textbf{rtsp}: Route to RTSP protocol analyzer.
- \textbf{sdp}: Route to SDP protocol analyzer.
- \textbf{secure-http}: Route to secure HTTP protocol analyzer.
- \textbf{sip \{ advanced \}}: Route to SIP protocol analyzer.

For SIP calls to work with NAT/Stateful Firewall, a SIP ALG is required to do payload translation of SIP packets and pin-hole (dynamic flow) creation for media packets. A SIP routing rule must to be configured for routing the packets to the SIP ALG for processing. If the optional keyword \texttt{advanced} is configured, the packets matching the routing rule will be routed to SIP ALG for processing and not to ECS SIP analyzer. If not configured, then packets will be routed to ECS SIP analyzer for processing.

Also, see \texttt{firewall nat-alg} CLI command in the ACS Configuration Mode.

- \textbf{tftp}: Route to TFTP protocol analyzer.
- \textbf{smtp}: Route to SMTP protocol analyzer.
- \textbf{wsp-connection-less}: Route to WSP connection-less protocol analyzer.
- \textbf{wsp-connection-oriented}: Route to WSP connection-oriented protocol analyzer.

\textbf{Important}: To route packets to the P2P analyzer, the ruledef should have rules to match all IP packets. Otherwise, the analyzer may not detect all P2P traffic.

\textbf{Important}: Use the \texttt{show active-charging analyzer statistics} command in the Exec Mode to see the list of supported analyzers.

\texttt{description description}

Enables to add a description to the rule and action for later reference in saved configuration file. \textit{description} must be an alpha and/or numeric string of 1 through 63 characters in length.

\textbf{Usage}

Instances of this CLI command control which packets are routed to which protocol analyzers. Packets sent to Active Charging are always passed through the IP protocol analyzer. This CLI command controls which higher layer analyzers are also invoked.

<table>
<thead>
<tr>
<th>Analyzer</th>
<th>Common ways to route to the analyzer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>All IPv4 packets are automatically routed here.</td>
</tr>
<tr>
<td>icmp</td>
<td>All IPv4 packets with IP protocol = ICMP (1) are automatically routed here.</td>
</tr>
<tr>
<td>tcp</td>
<td>All IPv4 packets with IP protocol = TCP (6) are automatically routed here.</td>
</tr>
<tr>
<td>udp</td>
<td>All IPv4 packets with IP protocol = UDP (17) are automatically routed here.</td>
</tr>
<tr>
<td>dns</td>
<td>UDP destination port or source port is DNS (53).</td>
</tr>
<tr>
<td>http</td>
<td>TCP destination port or source port is HTTP (80).</td>
</tr>
<tr>
<td>Analyzer</td>
<td>Common ways to route to the analyzer</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>secure-http</td>
<td>TCP destination port or source port is HTTPS (443). Note that HTTP may use the CONNECT method (see RFC 2817), in which case, the subscriber will be upgraded with transport layer security, but the traffic to/from the chassis will still be HTTP and be passed through the http rather than the secure-http analyzer (assuming that routing to the http analyzer has been configured).</td>
</tr>
<tr>
<td>wsp</td>
<td>UDP destination port or source port is connection-less WSP (9200) or connection-oriented WSP (9201).</td>
</tr>
<tr>
<td>wtp</td>
<td>Packets are automatically routed here, if you specified “wsp-connection-oriented” as described above.</td>
</tr>
<tr>
<td>wap2</td>
<td>TCP destination port or source port of the carrier-specific port number for WAP-2 (e.g. one carrier uses 8799); or, send all HTTP traffic to the wap2 analyzer if the carrier does not use a special port number.</td>
</tr>
<tr>
<td>ftp</td>
<td>TCP destination port or source port is FTP control (21) or FTP data (20); or, ftp analyzer (for FTP control packets) dynamically detected an FTP data flow over TCP (tcp dynamic-flow = ftp-data).</td>
</tr>
<tr>
<td>file-transfer</td>
<td>FTP and the command name is retr or stor; or, HTTP and the request method is get or post.</td>
</tr>
<tr>
<td>mms</td>
<td>WSP content type is application/vnd.wap.mms-message; or, WSP uri contains “mms”; or, HTTP content type is application/vnd.wap.mms-message; or, HTTP uri contains “mms”.</td>
</tr>
<tr>
<td>sip</td>
<td>UDP destination port or source port is SIP (5060).</td>
</tr>
<tr>
<td>sdp</td>
<td>RTSP or SIP content type is application/sdp</td>
</tr>
<tr>
<td>smtp</td>
<td>TCP destination port or source port is SMTP (25).</td>
</tr>
<tr>
<td>imap</td>
<td>TCP destination port or source port is IMAP (143).</td>
</tr>
<tr>
<td>pop3</td>
<td>TCP destination port or source port is POP3 (110).</td>
</tr>
<tr>
<td>rtp and rtcp</td>
<td>RTSP has embedded RTP/RTCP payloads (you need to enable RTP dynamic flow detection to catch those flows); or, RTSP or SDP (for SDP within SIP) creates an RTP/RTCP flow over UDP (in addition to enabling the aforementioned dynamic flow detection, you must make sure that UDP packets are routed to the UDP analyzer) or, RTP/RTCP uses predefined UDP port numbers (e.g. default UDP port numbers of 5004/5005).</td>
</tr>
<tr>
<td>rtsp</td>
<td>TCP destination port or source port is RTSP (554).</td>
</tr>
<tr>
<td>p2p</td>
<td>Use the <strong>p2p dynamic-flow-detection</strong> CLI command to enable detection of the different P2P applications specified by the <strong>p2p application</strong> CLI command; that will cause every TCP or UDP packet to be automatically routed here.</td>
</tr>
</tbody>
</table>

**Example**

The following command assigns a route and rule action with the route priority of 23, a ruledef of test, and an analyzer **test_analyzer** with description as **route_test1** to the current rulebase:

```
route priority 23 ruledef test analyzer test_analyzer description route_test1
```
rtp dynamic-flow-detection

This command enables the RTSP and SDP analyzers to detect the start/stop of RTP and RTCP flows.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ no | default ] rtp dynamic-flow-detection

no
Disables the previous RTP dynamic flow detection configuration.

default
Sets the default RTP dynamic flow detection configuration.
Default: no rtp dynamic-flow-detection

Usage
Use this command to enable the RTSP and SDP analyzer to detect the start/stop of RTP and RTCP flows. This command is used in conjunction with the route priority command.

Example
The following command enables RTP dynamic flow detection:

rtp dynamic-flow-detection
ruledef-parsing

This command configures whether to consider/ignore the port number embedded in the application header (for example, the "80" in www.starentnetworks.com:80) when comparing the ruledef expressions to the packet contents.

Product: ECS
Privilege: Security Administrator, Administrator
Syntax:

[ no ] ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }

default ruledef-parsing

no
Disables the previous configuration.

default
Sets the default configuration.
Default: no ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }—not ignoring port numbers that are embedded in application headers

ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }

Specifies to ignore the port numbers present in application header.
Specifies analyzers for which port number must be ignored.

Usage
Use this command to make the HTTP, RTSP, SIP, and WSP analyzer ignore port numbers embedded in application headers.

Example
The following command makes the HTTP analyzer in the current rulebase ignore port numbers embedded in application headers:

ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers http
tcp 2msl-timeout

This command configures how long to retain the TCP flow after the FIN has been acknowledged.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**
```
tcp 2msl-timeout seconds
{ default | no } tcp 2msl-timeout
```

- **default**
  Sets the default setting.
  Default: 2 seconds

- **no**
  Disables the timeout and sets the system to delete the flow immediately upon seeing the FIN be acknowledged.

- **seconds**
  The period of time, in seconds, to keep the TCP flow.
  seconds must be an integer from 1 through 20.

**Usage**
Use this command to configure how long to retain the TCP flow after the FIN has been acknowledged.
Acknowledgment to the FIN is not guaranteed to be received by the destination, then the FIN could be resent and re-acknowledged. In this scenario, it is desirable to still have the flow, so that the re-sends do not create a new flow.

**Example**
The following command sets the timeout to 4 seconds:
```
tcp 2msl-timeout 4
```
tcp check-window-size

This command enables/disables TCP window-size check.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ default | no ] tcp check-window-size
```

- **default**
  Sets the default setting.
  Default: enabled, i.e. packets after the erroneous packet (with size > receiver’s window size) will hit tcp-error ruledef.

- **no**
  Disables the window-size check, and will continue with normal L7 parsing.

**Usage**

Use this command to enable/disable TCP window-size check for packets out of TCP window.

**Example**

The following command enables TCP window-size check:

```
tcp check-window-size
```
tcp mss

This command configures the TCP Maximum Segment Size (MSS) in TCP SYN packets.

**Important:** This command is only available in StarOS 8.1 and later releases.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
tcp mss tcp_mss { add-if-not-present | limit-if-present } +
{ default | no } tcp mss
```

- **default**
  Removes the previously configured setting.

- **no**
  Removes the previously configured setting.

- **tcp_mss**
  Specifies the TCP MSS value.
  `tcp_mss` must be an integer from 496 through 65535.

- **add-if-not-present**
  Adds the TCP MSS if not present in the packet.

- **limit-if-present**
  Limits the TCP MSS if present in the packet.

**Usage**
Using this command, TCP MSS can be limited if already present in the TCP SYN packets. If there are no errors detected in IP header/TCP mandatory header and there are no mem allocation failures, TCP optional header is parsed. If TCP MSS is present in the optional header and its value is greater than the configured MSS value, the value present in the TCP packet is replaced with the configured one.
If the TCP optional header is not present in the SYN packet and there are no errors in already present TCP header, the TCP MSS value configured will be inserted while sending the current packet out.

**Example**
The following command limits the TCP maximum segment size to 3000, and if not present adds it to the packets:
```
tcp mss 3000 limit-if-present add-if-not-present
```
tcp out-of-order-timeout

**Description** This command has been deprecated, and is replaced by the tcp packets-out-of-order command.
tcp packets-out-of-order

This command configures processing of TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

tcp packets-out-of-order { timeout duration_ms | transmit [ after-reordering | immediately ] }

default tcp packets-out-of-order { timeout | transmit }

---

**timeout duration_ms**
Default: 5000 milliseconds
Specifies the timeout period for re-assembly of TCP out-of-order packets. duration_ms is the timeout period in milliseconds, and must be an integer from 100 through 30000.

---

**transmit [ after-reordering | immediately ]**
Configures the TCP out-of-order segment behavior after buffering a copy.

- **after-reordering**: Sends the TCP out-of-order segment after all packets are received and successfully reordered. If reordering is not successful due to a timeout, the received packets are forwarded without being passed through the protocol analyzers. If memory allocation fails or the received packet is partial retransmitted data, the packet will be forwarded immediately without being passed through the protocol analyzers, except for the IP analyzer.

- **immediately**: Sends the TCP out-of-order segment immediately after buffering a copy. The packets are transmitted as they are received without any in-line services or charging action processing, but also a copy of each packet is held onto. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded.

Default: **immediately**

---

**Usage**
This command configures how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

**Example**
The following command sets the timeout timer to 10000 milliseconds:
tcp packets-out-of-order timeout 10000
timestamp rounding

This command enables the configuration of timestamp rounding in an EDR or eG-CDR.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
timestamp rounding { edr | egcdr } { ceiling | floor | round-off }
{ no | default } timestamp rounding { edr | egcdr }
```

```
no | default
Default: round-off
Sets the default setting for timestamp rounding.
```

```
edr
Perform the timestamp rounding for EDRs.
```

```
egcdr
Perform the timestamp rounding for eG-CDRs.
```

```
floor
This keyword always discards the fractional part of the second.
```

```
round-off
This keyword sets the fractional part of the seconds to nearest integer value. If fractional value is greater than or equal to 0.5, it adds 1 to the number of seconds and discards the fractional part of second.
```

Usage
Use this command to configure the timestamp rounding setting. The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (i.e., 2 \(\times\) 1 = 1). This command may be repeated for each type of EDR or eG-CDR.

Example
The following command sets the EDR timestamp to nearest integer value second; i.e. 34:12.23 to 34:12.00:
```
timestamp rounding edr round-off
```
transport-layer-checksum

This command enables/disables checksum verification for TCP and UDP packets.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

[ no ] transport-layer-checksum verify-during-packet-inspection [ tcp | udp ]

default transport-layer-checksum

no
Disables the checksum calculation for the specified packet type.

default
Sets the default configuration.
Default: transport-layer-checksum verify-during-packet-inspection—to perform the checksum verification calculation on all TCP and UDP packets.

[ tcp | udp ]
Specifies that either TCP or UDP packets should be verified or not verified.
If neither of these keywords is specified the command applies to both TCP and UDP packets.

Usage
Use this command to disable or enable performing checksum verification calculations on TCP or UDP packets.
If the checksum is not verified, the packets will go through the TCP/UDP analyzers (and deeper analyzers, if so configured with the route CLI command) regardless of the value of the TCP/UDP checksum.
If the checksum is verified, only packets with good checksums will go through the TCP/UDP analyzers (and deeper analyzers, if so configured).

Example
The following command disables checksum verification calculations on all TCP and UDP packets:

no transport-layer-checksum verify-during-packet-inspection
udr threshold

This command defines and enables the threshold limit to generate User Detail Records (UDRs) that provide Comma Separated Value (CSV) records written periodically in a fixed schema designed to reflect a total billable quantity.

Product
All

Privilege
Security Administrator, Administrator

Syntax

udr threshold { interval interval | volume { downlink bytes [ uplinkbytes] | totalbytes| downlinkbytes[ uplinkbytes] }}

default udr threshold { interval | volume }

no udr threshold { interval | volume { downlink [ uplink ] | total | uplink [ downlink ] } }

no
Removes the previous configuration.

default
Sets the default configuration.
Default: no udr threshold interval: no udr threshold volume—disables the UDR threshold settings.

interval interval
Default: 0 (Disabled)
Specifies the time interval in seconds for closing the UDR if the minimum time duration thresholds are satisfied. This option is disabled by default.
interval must be an integer from 60 through 40000000.

volume
Specifies the uplink/downlink volume octet counts for the generation of the interim UDRs.

• downlink bytes: Sets the limit for the number of octets downlink after which the UDR is closed. bytes (in bytes) must be an integer from 100,000 to 4,000,000,000. Default is 4,000,000,000.

• total bytes: Sets the limit for the total number of octets (uplink+downlink) after which the UDR is closed. bytes (in bytes) must be an integer from 100,000 to 4,000,000,000. By default, this configuration is disabled.

• uplink bytes: Sets the limit for the number of octets uplink after which the UDR is closed. bytes (in bytes) must be an integer from 100,000 through 4,000,000,000. Default is 4,000,000,000.

UDR records are generated whenever either threshold is reached.
Use this command to enable the thresholds for generation of UDRs.

Example
The following command specifies that UDR records should be generated every 10 minutes (600 seconds):

```
udr threshold interval 600
```
.udr trigger

Use this command to assign first packet trigger to interim UDRs—for generating UDR for first packet hit per rating group/content ID.

Important: This command is only available in StarOS 8.3 and later.

Product
ACS

Privilege
Security Administrator, Administrator

Syntax

[ no ] udr trigger first-hit-content-id

default udr trigger

no
Disables assigning first packet trigger to interim UDRs.

default
Configures the default setting.
Default: Disabled

first-hit-content-id
Specifies interim UDR generation on first packet hit per rating group/content ID.

Usage
This command enables generating UDR for first packet hit per rating group/content ID. Generation of UDR will be triggered when this CLI command is present in the rulebase.

Example
The following command assigns first packet trigger to interim UDRs, for generating UDR for first packet hit per rating group/content ID:

.udr trigger first-hit-content-id
url-blacklisting action

This command enables/disables URL Blacklisting functionality for the rulebase, and configures the action to be taken when a URL matches one in the URL Blacklist.

Product
ECS, CF

Privilege
Security Administrator, Administrator

Syntax
url-blacklisting action { discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ edr ]

{ default | no } url-blacklisting action

- [ default | no ] url-blacklisting action
  Disables the URL Blacklisting feature for this rulebase.

- discard
  Configures URL Blacklisting discard action.

- redirect-url url
  Configures URL Blacklisting redirect-url action.
  url specifies the redirect URL/URI. url must be a fully qualified URL/URI, and must be a string of 1 through 1023 characters in length.

- terminate-flow
  Configures URL Blacklisting terminate-flow action.

- www-reply-code-and-terminate-flow reply_code
  Configures URL Blacklisting terminate-flow action with reply code.
  reply_code specifies the reply code, and must be an integer from 100 through 599.

Usage
Use this command to enable/disable URL Blacklisting functionality, and configure the EDRs to be generated on Blacklisting match and the action to be taken.

Example
The following command enables URL Blacklisting functionality, and configures the terminate-flow action with reply code 300:
url-blacklisting action www-reply-code-and-terminate-flow 300
The following command disables URL Blacklisting feature in the rulebase:
no url-blacklisting action
url-preprocessing

This command enables/disables a group-of-prefixed-urls for preprocessing.

**Important:** This command is customer specific. For more information, please contact your local service representative.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] url-preprocessing bypass group-of-prefixed-urls group_name
```

- **no**
  - Removes configuration for the specified group-of-prefixed-urls.

- **group_name**
  - Specifies the group-of-prefixed-urls name.
  - `group_name` must be an alpha and/or numeric string of 1 through 63 characters in length.

**Usage**

Use this command to enable/disable a group-of-prefixed-urls. Multiple groups can be enabled.

**Example**

The following command enables looking for prefixed URLs of the group-of-prefixed-urls named `test5`:

```
url-preprocessing bypass group-of-prefixed-urls test5
```
wtp out-of-order-timeout

**Description** This command has been deprecated, and is replaced by the `wtp packets-out-of-order` command.
**wtp packets-out-of-order**

This command configures how to process WTP packets that are out of order, while waiting for the earlier packet(s) to arrive.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```
wtp packets-out-of-order { out-of-order-timeout timeout | transmit [ after-reordering | immediately ] }  
default wtp packets-out-of-order { out-of-order-timeout | transmit }  
default
```

**default**
Configures the default setting.

**out-of-order-timeout timeout**

Specifies the maximum duration for which WTP out-of-order packets are retained, in milliseconds, before reassembly is needed.

- **timeout** is the timeout duration in milliseconds, and must be an integer from 100 through 30000.
- Default: 5000 milliseconds

**transmit [ after-reordering | immediately ]**

Specifies the WTP out-of-order segment behavior after buffering a copy:

- **after-reordering**: Send WTP out-of-order segment after it becomes ordered
- **immediately**: Send WTP out-of-order segment immediately after buffering a copy
- Default: **immediately**

**Usage**

Use this command to configure TCP out-of-order segment options.

- If out-of-order-timeout is specified, out-of-order packets are retained, until either all packets have been received or the configured timeout has expired for the oldest packet. If all packets have been received, a temporary complete packet is reconstructed for analysis. Then all packets are forwarded in order from first to last. If all packets are not received, the packets will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.
- If **after-reordering** transmitting is specified, the packets are held onto and reordered. After successfully reordering the packets, they are processed in the proper order. If reordering is not successful due to timeout (wtp out-of-order-timeout), the received packets are forwarded without being passed through the protocol analyzers.
- If **immediately** is specified, the packets are transmitted as they are received without any in-line services or Charging Action processing, however a copy of each packet is retained. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is undertaken, and then the last packet is forward (unless otherwise configured by the in-line services or Charging Action).
Example
The following command sets the timeout timer to 10000 milliseconds:

```
wtp out-of-order-timeout 10000
```
xheader-encryption

This command configures X-Header Encryption feature parameters.

⚠️ **Important:** This command is license dependent. For more information, please contact your local sales representative.

**Product**
ECS

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
xheader-encryption { certificate-name certificate_name | re-encryption period period }

default xheader-encryption re-encryption period

no xheader-encryption { certificate-name | re-encryption }
```

**default**
Configures the default setting.
Default: no re-encryption

**no**
Removes the previously configured setting for the specified parameter.

**certificate-name certificate_name**
Specifies name of the encryption certificate to be used for X-Header Encryption feature.
*certificate_name* must be the name of a certificate, and must be an alpha and/or numeric string of 1 through 63 characters in length.

**re-encryption period**
Specifies how often to re-generate the encryption keys.
*period* specifies the re-encryption time period in minutes, and must be an integer from 1 through 10000.

**Usage**
Use this command to configure the X-Header Encryption feature’s certificate and re-encryption parameters.

**Example**
The following command configures the X-Header Encryption feature to use the certificate named *testcert*:

```
xheader-encryption certificate-name testcert
```
Chapter 182
Ruledef Configuration Mode Commands

The Ruledef Configuration Mode is used to create and manage ACS rule definitions.

**Important:** Up to 10 rule matches can be configured in one ruledef.

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

The following commands define rules for analyzing traffic based on the bearer channel:
**bearer 3gpp apn**

This command defines a rule definition to analyze and charge user traffic based on APN of the bearer flow.

---

**Important:** This command is only available in StarOS 8.1 and later.

---

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer 3gpp apn [ case-sensitive ] operator value
```

- **no**
  - Removes the specified rule definition.

- **[ case-sensitive ]**
  - Default: Disabled
  - This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - *operator* must be one of the following:
    - `!=`: does not equal
    - `!contains`: does not contain
    - `!ends-with`: does not end with
    - `!starts-with`: does not start with
    - `=`: equals
    - `contains`: contains
    - `ends-with`: ends with
    - `starts-with`: starts with

- **value**
  - The name of the matching APN in bearer flow.
  - *value* must be an alpha and/or numeric string of 1 through 62 characters in length, and can contain punctuation characters.

---

**Usage**

Use this command to specify a rule definition to analyze user traffic based on APN of the bearer flow.
Example
The following command creates a rule definition to analyze user traffic for an APN named \texttt{apn12}:

\begin{verbatim}
bearer 3gpp apn = apn12
\end{verbatim}
bearer 3gpp imsi

This command defines a rule definition to analyze and charge user traffic based on the International Mobile Station Identification number (IMSI) in bearer flow.

**Important:** This command is only available in StarOS 8.1 and later.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer 3gpp imsi { operator imsi | { !range | range } imsi-pool imsi_pool }
```

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the IMSI.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **imsi**
  - Specifies the mobile station identifier.

- `{ !range | range } imsi-pool imsi_pool`
  - `!range` | `range`: Specifies the range criteria:
    - `!range`: Not in the range of
    - `range`: In the range of

  - `imsi-pool imsi_pool`: Specifies the IMSI pool name. `imsi_pool` must be a string of 1 through 63 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on IMSI.

**Example**

The following command creates a rule definition to analyze user traffic for the IMSI number 9198838330912:

```
bearer 3gpp imsi = 9198838330912
```
bearer 3gpp imsi
bearer 3gpp rat-type

This command defines a rule definition to analyze and charge user traffic based on the Radio Access Technology (RAT) in bearer flow.

**Important:** This command is only available in StarOS 8.1 and later.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] bearer 3gpp rat-type operator rat
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **rat**
  The rat type associated with the bearer flow.
  - `geran`: GSM EDGE Radio Access Network type
  - `utran`: UMTS Terrestrial Radio Access Network type
  - `wlan`: Wireless LAN type

Usage
Use this command to specify a rule definition to analyze user traffic based on RAT type.

Example
The following command creates a rule definition for analyzing user traffic for the WLAN RAT type `wlan`:

```
bearer 3gpp rat-type = wlan
```
bearer 3gpp sgsn-address

This command defines a rule definition to analyze and charge user traffic based on SGSN address associated in 3gpp bearer flow.

**Important:** This command is only available in StarOS 8.1 and later.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] bearer 3gpp sgsn-address operator address
```

**no**
Removes the specified rule definition.

**operator**
Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
- `!=`: does not equal
- `==`: equals

**address**
Specifies IP address of the SGSN node. `address` must be an SGSN IP address expressed in standard IPv4 or IPv6 dotted decimal notation.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on IP address of SGSN node. This command replaces the `bearer sgsn-address` command.

**Example**
The following command creates a rule definition for analyzing traffic for an SGSN node with IP address of `19.88.3.8`.

```plaintext
bearer 3gpp sgsn-address = 19.88.3.8
```
bearer 3gpp2 bsid

This command defines a rule definition to analyze and charge user traffic based on the 3GPP2 service Base Station Identifier (BSID) for bearer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] bearer 3gpp2 bsid [ case-sensitive ] operator bs_id

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  - !: does not equal
  - !contains: does not contain
  - !ends-with: does not end with
  - !starts-with: does not start with
  - ==: equals
  - contains: contains
  - ends-with: ends with
  - starts-with: starts with

- **bs_id**
  The name of the matching 3GPP2 service Base Station ID (BSID) in bearer flow.
  bs_id must be an alpha and/or numeric string of 1 through 12 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on 3GPP2 service Base Station Identifier (BSID).

Example
The following command creates a rule definition for analyzing user traffic for a 3GPP2 BSID named `bs001_xyz`:

```
bearer 3gpp2 bsid = bs001_xyz
```
bearer 3gpp2 service-option

This command defines a rule definition to analyze and charge user traffic based on the 3GPP2 service with service options for bearer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
[ no ] bearer 3gpp2 service-option operator option_code
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: does not equal</td>
</tr>
<tr>
<td>• &lt;=: less than or equals</td>
</tr>
<tr>
<td>• =: equals</td>
</tr>
<tr>
<td>• &gt;=: more than or equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>option_code</th>
</tr>
</thead>
<tbody>
<tr>
<td>The code of the matching 3GPP2 service option in bearer flow.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>option_code</th>
</tr>
</thead>
<tbody>
<tr>
<td>option_code must be an integer from 0 through 1000.</td>
</tr>
</tbody>
</table>

Usage
Use this command to specify a rule definition to analyze user traffic based on 3GPP2 service’s service option code.

Example
The following command creates a rule definition for analyzing user traffic for a 3GPP2 service’s service option as = 1034:

```bash
bearer 3gpp2 service-option = 1034
```
bearer apn

This command defines a rule definition to analyze and charge user traffic based on APN bearer.

**Important:** In StarOS 8.1 and later, this command is deprecated and is replaced by the `bearer 3gpp apn` command.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer apn [ case-sensitive ] operator value
```

- **no**
  Removes the specified rule definition.

- **[ case-sensitive ]**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **value**
  The name of the matching APN in bearer flow.
  `value` must be an alpha and/or numeric string of 1 through 62 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on APN name.
Example
The following command creates a rule definition for analyzing user traffic for an APN name `apn12`:

```
bearer apn = apn12
```
bearer imsi

This command defines a rule definition to analyze and charge user traffic based on International Mobile Station Identification number (IMSI) in bearer flow.

**Important:** In StarOS 8.1 and later, this command is deprecated and is replaced by the `bearer 3gpp imsi` command.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer imsi { operator imsi | { !range | range } imsi-pool imsi_pool }
```

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the IMSI.
  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **msid**
  - Specifies the Mobile Station Identifier.

- `{ !range | range } imsi-pool imsi_pool`
  - **!range | range**: Specifies the range criteria:
    - `!range`: Not in the range of
    - `range`: In the range of
  - **imsi-pool imsi_pool**: Specifies the IMSI pool name. `imsi_pool` must be a string of 1 through 63 characters in length.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on IMSI number of mobile station.

**Example**
The following command creates a rule definition to analyze user traffic for an IMSI number `9198838330912`:

```
bearer imsi = 9198838330912
```
bearer rat-type

This command defines a rule definition to analyze and charge user traffic based on the Radio Access Technology (RAT) in bearer flow.

**Important:** In StarOS 8.1 and later, this command is deprecated and is replaced by the `bearer 3gpp rat-type` command.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer rat-type operator rat
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!eq`: does not equal
  - `eq`: equals

- **rat**
  The rat type associated with the bearer flow.
  - `geran`: GSM EDGE Radio Access Network type
  - `utran`: UMTS Terrestrial Radio Access Network type
  - `wlan`: Wireless LAN type

**Usage**
Use this command to specify a rule definition to analyze user traffic based on RAT type.

**Example**
The following command creates a rule definition for analyzing user traffic for the WLAN RAT type `wlan`:

```
bearer rat-type = wlan
```
bearer sgsn-address

This command defines a rule definition to analyze and charge user traffic based on SGSN address associated in bearer flow.

**Important:** In StarOS 8.1 and later, this command is deprecated and is replaced by the `bearer 3gpp sgsn-address` command.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] bearer sgsn-address operator address
```

**no**
Removes the specified rule definition.

**operator**
Specifies how to logically match the information in the analyzed field.

*`operator`* must be one of the following:
- `!=`: does not equal
- `=`: equals

**address**
The IP address of SGSN node.

*`address`* must be an SGSN IP address expressed in standard IPv4 or IPv6 notation.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on IP address of SGSN node.

**Example**
The following command creates a rule definition for analyzing user traffic for an SGSN node with IP address of 19.88.3.8:

```
bearer sgsn-address = 19.88.3.8
```
bearer traffic-group

This command defines a rule definition to analyze and charge user traffic based on the traffic group number associated to the bearer flow.

**Important:** This functionality is only available if the license for Content Access Control (P/N: 699-00-0011) has been purchased and installed.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] bearer traffic-group operator grp_num
```

- **no**
  
  Removes the specified rule definition.

- **operator**
  
  Specifies how to logically match the information in the analyzed field. **operator** must be one of the following:
  
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **grp_num**
  
  Specifies the traffic group number. **grp_num** must be an integer from 1 through 255.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the traffic group value. See the **fa-ha-spi** command in the **HA Service Configuration Mode Commands** chapter for more information.

**Example**

The following command creates a rule definition for all traffic groups assigned a value greater or equal to 23:

```
bearer traffic-group >= 23
```
The following commands define rules for packets based on Credit Control Application:


cca quota-state

This command specifies the quota state of a subscriber for prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] cca quota-state operator { limit-reached | lower-bandwidth }

    no
    Disables the configured credit control quota state for this rule definition.

    operator
    Specifies how to logically match the information in the analyzed field. operator must be one of the following:
        ● !=: does not equal
        ● <=: lesser than equal
        ● ==: equals
        ● >=: greater than equal

    limit-reached
    This state matches an affirmative end-of-quota indication for this rule definition from the prepay server.

    lower-bandwidth
    This state matches the lower-bandwidth quota state of a rating group.

Usage
This command supports URL redirection cases and creates a rule for subscriber prepaid quota state as exhausted or not exhausted.
If a subscriber has exhausted the quota but has not exhausted the qualified period, a different charging-action can applied based on the cca quota-state CLI.

Example
The following command creates a rule for subscriber to send end-of-quota indication when credit control prepay quota limit reached:

    cca quota-state = limit-reached
cca redirect-indicator

This command configures the value of the redirect-indicator state of the credit control application.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] cca redirect-indicator operator indicator
```

- **no**
  Disables the configured credit control redirect indicator for specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - !=: does not equal
  - <=: less than or equals
  - ==: equals
  - >=: greater than or equals

- **indicator**
  Specifies the redirect indicator for AVP used for redirection of URL in RADIUS dictionary used for prepaid service.
  **indicator** must be an integer from 0 through 4294967295.

**Important:** For the RADIUS server configured with different values to return for this AVP the ECS requires rule definitions to match the different values for system to associate with Charging Actions that have different redirect URLs configured.

**Usage**

This command is used to configure an AVP to be used from a dictionary that defines the AVP for the redirect-indicator.

For example, a RADIUS dictionary specifies the 3gpp2-release-indicator to be used for redirect indicator when RADIUS is used as the credit control application. In this case, the value for 3gpp2-release-indicator that is returned by the RADIUS prepaid server for a quota request for a given content-id is retained by system and associated with the flow.

**Example**

Following command specifies redirect indicator as 1234 for URL redirect AVP:
cca redirect-indicator = 1234
copy-packet-to-log

This command prints every packet that hits this rule to a log statement.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] copy-packet-to-log

no
Disables the feature.
```

**Usage**
Use this command to print every packet that hits this rule to a log statement.
The following commands define rules for packets based on the DNS:
**dns answer-name**

This command defines a rule definition to analyze and charge user traffic based on the DNS answer-name.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] dns answer-name [ case-sensitive ] operator value
```

**no**
Removes the specified rule definition.

**case-sensitive**
Default: Disabled
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

**operator**
Specifies how to logically match the information in the analyzed field.
- `!=`: does not equal
- `!contains`: does not contain
- `!ends-with`: does not end with
- `!starts-with`: does not start with
- `=`: equals
- `contains`: contains
- `ends-with`: ends with
- `starts-with`: starts with

**value**
The value of the specified field.
**value** must be an alpha and/or numeric string of 1 through 255 characters in length, and can contain punctuation characters.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on answer name.

**Example**
The following command creates a rule definition for analyzing user traffic for a answer name of `test`:
dns answer-name = test
dns any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for DNS packets.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] dns any-match operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- ! =: does not equal
- = : equals

condition
Specifies the condition for this rule definition. condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to specify an any match rule definition for analyzing user traffic for charging purposes.

Example
The following command defines an any match rule definition for analyzing DNS user traffic:

```bash
dns any-match = TRUE
```
dns previous-state

This command defines a rule definition to analyze and charge user traffic matching the previous state expressions for DNS packets.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] dns previous-state operator dns_state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !: does not equal
• =: equals

dns_state
dns_state must be one of the following:
• dns-timeout
• init
• req-sent
• resp-error
• resp-success

Usage
Use this command to specify a rule definition to analyze user traffic based on the DNS previous state.

Example
The following command creates a rule definition for analyzing user traffic using a previous state of req-sent:

dns previous-state = req-sent
dns query-name

This command defines a rule definition to analyze and charge user traffic based on the DNS query-name.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] dns query-name [ case-sensitive ] operator value

no
Removes the specified rule definition.

case-sensitive
Default: Disabled
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • !=: does not equal
  • !=contains: does not contain
  • !=ends-with: does not end with
  • !=starts-with: does not start with
  • =: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

value
The value of the specified field.
value must be an alpha and/or numeric string of 1 through 255 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on the DNS query name.

Example
The following command creates a rule definition for analyzing user traffic using a query name of test:
dns query-name = test


dns return-code

This command defines a rule definition to analyze and charge user traffic based on the DNS return-code.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] dns return-code operator dns_response
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **dns_response**
  `dns_response` must be one of the following:
  - `format-error`
  - `name-error`
  - `no-error`
  - `not-implemented`
  - `refused`
  - `server-failure`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a DNS return code.

**Example**
The following command creates a rule definition for analyzing user traffic using a DNS response of `refused`:

```
dns return-code = refused
```
**dns state**

This command defines a rule definition to analyze and charge user traffic based on the DNS state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] dns state operator dns_state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **dns_state**
  **dns_state** must be one of the following:
  - `dns-timeout`
  - `init`
  - `req-sent`
  - `resp-error`
  - `resp-success`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a DNS state.

**Example**
The following command creates a rule definition for analyzing user traffic using a DNS state of `req-sent`:

```
dns state = req-sent
```
**dns tid**

This command defines a rule definition to analyze and charge user traffic based on the DNS Transaction Identifier (TID).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] dns tid operator tid_value
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **tid_value**
  Specifies the DNS transaction identifier for this rule definition. `tid_value` must be an integer from 1 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the DNS TID.

**Example**

The following command creates a rule definition for analyzing user traffic using a DNS TID value of `test`:

```
dns tid = test
```
email

This command defines a rule definition to analyze and charge user traffic based on the conditions based on e-mail parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] email { cc | content { class | type } | from | size | subject | to } [ case-sensitive ] operator value
```

- **no**
  Removes the specified rule definition.

- **cc**
  Specifies to match on the information in the CC field of e-mail message.

- **content { class | type }**
  Specifies to match on the information in the “content-type” or “content-class” field of e-mail message.

- **from**
  Specifies to match on the information in the “from” field of e-mail message.

- **subject**
  Specifies to match on the information in the “subject” field of e-mail message.

- **to**
  Specifies to match on the information in the “to” field of e-mail message.

- **size**
  Specifies to match with the total size of e-mail message in bytes.

- **case-sensitive**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field of e-mail message.
  - `!=`: does not equal
  - `!contains`: does not contain
**email**

- `!ends-with`: does not end with
- `!starts-with`: does not start with
- `=`: equals
- `contains`: contains
- `ends-with`: ends with
- `starts-with`: starts with

*operators* must be one of the following for *size*:
- `!=`: does not equal
- `<=`: less than or equals
- `=`: equals
- `=>`: greater than or equals

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The value of the specified field. <em>value</em> must be an alpha and/or numeric string (allows punctuation characters) as follows:</td>
</tr>
<tr>
<td>• <strong>cc</strong>: A string of 1 through 512 characters in length</td>
</tr>
<tr>
<td>• <strong>content</strong>: A string of 1 through 128 characters in length</td>
</tr>
<tr>
<td>• <strong>from</strong>: A string of 1 through 64 characters in length</td>
</tr>
<tr>
<td>• <strong>size</strong>: A range of bytes from 1 through 400000000 bytes</td>
</tr>
<tr>
<td>• <strong>subject</strong>: A string of 1 through 128 characters in length</td>
</tr>
<tr>
<td>• <strong>to</strong>: A string of 1 through 512 characters in length</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to specify a rule definition to analyze user traffic based on different fields and parameters of e-mail message.

**Example**

The following command creates an email rule definition for analyzing user traffic for the occurrence of triangular in the ‘cc’ field of e-mail message:

```
email cc contains triangular@xyz.com
```
end

This command returns the CLI prompt to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to change to the Exec mode.
exit

This command exits the Ruledef Configuration mode and returns to the Active Charging Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the Active Charging Configuration mode.
file-transfer

The following commands define rules for analyzing traffic based on file transfers:
file-transfer any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for file transfer.

Product  
All

Privilege  
Security Administrator, Administrator

Syntax  

```plaintext
[ no ] file-transfer any-match operator condition
```

- **no**  
  Removes the specified rule definition.

- **operator**  
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `! =`: does not equal
  - `= =`: equals

- **condition**  
  Specifies the condition for this rule definition. 
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

Usage  
Use this command to specify a rule definition to analyze user traffic based on the file transfer any match status.

Example  
The following command creates a file transfer rule definition for analyzing user traffic using a file transfer any match status of `FALSE`:

```plaintext
file-transfer any-match = FALSE
```
**file-transfer chunk-number**

This command defines a rule definition to analyze and charge user traffic based on number of chunks in a file transfer.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] file-transfer chunk-number operator value
```

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
</tr>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
</tr>
<tr>
<td>Specifies how to logically match the information in the analyzed field. operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: does not equal</td>
</tr>
<tr>
<td>• &lt;==: less than or equals</td>
</tr>
<tr>
<td>• ==: equals</td>
</tr>
<tr>
<td>• &gt;=: greater than or equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
</tr>
<tr>
<td>Specifies the number of chunks for this rule definition. value must be an integer from 1 through 65535.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the number of chunks in a file transfer.

**Example**
The following command creates a file transfer rule definition for analyzing user traffic using 150 number of chunks:

```
file-transfer chunk-number = 150
```
file-transfer current-chunk-length

This command defines a rule definition to analyze and charge user traffic based on length of current chunk in a file transfer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] file-transfer current-chunk-length \{ operator \} \{ value \}

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- ! =: does not equal
- <=: less than or equals
- :=: equals
- >=: greater than or equals

value
Specifies the length in bytes of current chunk for this rule definition. value must be an integer from 1 through 4000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on the length of current chunk in a file transfer.

Example
The following command creates a file transfer rule definition for analyzing user traffic using current length of chunk as 150000 bytes:

file-transfer current-chunk-length = 150000
file-transfer declared-chunk-length

This command defines a rule definition to analyze and charge user traffic based on declared length of chunk in a file transfer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] file-transfer declared-chunk-length operator value

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- • ! =: does not equal
- • < =: less than or equals
- • = =: equals
- • > =: greater than or equals

value
Specifies the declared length, in bytes, of chunk for this rule definition.
value must be an integer from 1 through 4000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on the declared length of chunk in a file transfer.

Example
The following command creates a file transfer rule definition for analyzing user traffic using declared length of chunk as 2500000 bytes:

file-transfer declared-chunk-length = 2500000
file-transfer declared-file-size

This command defines a rule definition to analyze and charge user traffic based on declared size of file in a file transfer.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] file-transfer declared-file-size operator size
```

`no`
Removes the specified rule definition.

`operator`
Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
- `!`: does not equal
- `<=`: less than or equals
- `=`: equals
- `>=`: greater than or equals

`size`
Specifies the declared size of file, in bytes, for this rule definition. `size` must be an integer from 1 through 40000000.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the declared size of file in a file transfer.

**Example**
The following command creates a file transfer rule definition for analyzing user traffic using declared size of file as 2500000 bytes:

```
file-transfer declared-file-size = 2500000
```
file-transfer filename

This command defines a rule definition to analyze and charge user traffic based on declared name of the file in a file transfer.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] file-transfer filename [ case-sensitive ]operator size
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!=contains`: does not contain
  - `!=ends-with`: does not end with
  - `!=starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  Specifies the string for this rule definition.
  `string` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the declared name of file in a file transfer.

**Example**

```
The following command creates a file transfer rule definition for analyzing user traffic using declared name of file as *star1*:

```
file-transfer filename contains star1
```
file-transfer previous-state

This command defines a rule definition to analyze and charge user traffic based on the previous state of file transfer.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] file-transfer previous-state operator previous_state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • !=: does not equal
  • ==: equals

previous_state
previous_state must be one of the following:
  • init: Specifies previous state as initialization.
  • request-sent: Specifies previous state as request sent.
  • transfer-error: Specifies previous state as transfer error.
  • transfer-ok: Specifies previous state as transfer ok.

Usage
Use this command to specify a rule definition to analyze user traffic based on a previous state of file transfer.

Example
The following command creates a file transfer rule definition for analyzing user traffic using a previous file transfer state of init:

    file-transfer previous-state = init
file-transfer state

This command defines a rule definition to analyze and charge user traffic based on the current state of file transfer Finite State Machine (FSM).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] file-transfer state operator state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- ==: equals

state
state must be one of the following
- init: Specifies current state as initialization.
- request-sent: Specifies current state as request sent.
- transfer-error: Specifies current state as transfer error.
- transfer-ok: Specifies current state as transfer ok.

Usage
Use this command to specify a rule definition to analyze user traffic based on state of file transfer. Following table describes the details of file transfer FSM states with event:

<table>
<thead>
<tr>
<th>Event</th>
<th>init</th>
<th>request-sent</th>
<th>transfer-ok</th>
<th>transfer-err</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP &quot;RETR&quot; command or HTTP &quot;GET&quot; request received with chunk encoding</td>
<td>request-sent</td>
<td>Discarded</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
<tr>
<td>HTTP 2xx response received</td>
<td>transfer-ok</td>
<td>Discarded</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
<tr>
<td>HTTP 4xx or HTTP 5xx response received</td>
<td>transfer-error</td>
<td>Discarded</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
<tr>
<td>FTP reply received with reply status as file transfer complete/successful</td>
<td>Discarded</td>
<td>transfer-ok</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
<tr>
<td>FTP reply received with reply status as file transfer unsuccessful</td>
<td>Discarded</td>
<td>transfer-error</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
</tbody>
</table>
Example
The following command creates a file transfer rule definition for analyzing user traffic using a file transfer state of
init:

```
file-transfer state = init
```
file-transfer transferred-file-size

This command defines a rule definition to analyze and charge user traffic based on transferred size of file in a file transfer.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] file-transfer transferred-file-size operator size
```

- `no`
  - Removes the specified rule definition.

- `operator`
  - Specifies how to logically match the information in the analyzed field.
    - `operator` must be one of the following:
      - `!=`: does not equal
      - `<=`: less than or equals
      - `=`: equals
      - `>=`: greater than or equals

- `size`
  - Specifies the transferred size of file, in bytes, for this rule definition.
    - `size` must be an integer from 1 through 4000000000.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the transferred size of file in a file transfer.

**Example**

The following command creates a file transfer rule definition for analyzing user traffic using transferred size of file as 2500:

```
file-transfer transferred-file-size = 2500
```
ftp

The following commands define rules for analyzing traffic based on File Transfer Protocol (FTP):
ftp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for FTP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ftp any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `! =`: does not equal
  - `= =`: equals

- **condition**
  Specifies the condition for this rule definition. `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the FTP any match status.

**Example**

The following command creates an FTP rule definition for analyzing user traffic using an FTP any match status of `FALSE`:

```
ftp any-match = FALSE
```
ftp client-ip-address

This command defines a rule definition to analyze and charge user traffic based on FTP client IP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ftp client-ip-address operator ip_address
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **ip_address**
  `ip_address` must be the client’s IP address expressed in IPv4 dotted decimal or IPv6 colon notation.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on an FTP client IP.

**Example**
The following command creates an FTP rule definition for analyzing user traffic using a client IP of `1.1.1.1`:

```
ftp client-ip = 1.1.1.1
```
ftp client-port

This command defines a rule definition to analyze and charge user traffic based on FTP client port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ftp client-port operator port
```

- `no`
  Removes the specified rule definition.
- `operator`
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `==>`: greater than or equals
- `port`
  Specifies the port number for this rule definition. `port` must be an integer from 1 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an FTP client port.

**Example**

The following command creates an FTP rule definition for analyzing user traffic using ftp client port 10:

```
ftp client-port = 10
```
ftp command args

This command defines a rule definition to analyze and charge user traffic based on FTP command argument.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp command args [ case-sensitive ] operator argument

no
Removes the specified rule definition.

case-sensitive
Default: Disabled
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• !contains: does not contains
• !ends-with: does not end with
• !starts-with: does not start with
• =: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

argument
Specifies the argument for this rule definition.
argument must be a string of 1 through 127 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on an FTP command argument.

Example
The following command creates an FTP rule definition for analyzing user traffic using an FTP command argument of test:
ftp command args = test
**ftp command id**

This command defines a rule definition to analyze and charge user traffic based on FTP command ID.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ftp command id [ operator command_id ]
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **command_id**
  Specifies the command identifier for this rule definition.
  In StarOS 9.0 and later, `command_id` must be an integer from 0 through 18.
  In StarOS 8.3 and earlier, `command_id` must be an integer from 0 through 15.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an FTP command ID.

**Example**

The following command creates an FTP rule definition for analyzing user traffic using an FTP command ID of 10:

```
ftp command id = 10
```
ftp command name

This command defines a rule definition to analyze and charge user traffic based on FTP command name.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] ftp command name operator command_name
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator must be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• !=: does not equal</td>
</tr>
<tr>
<td>• ==: equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>command_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the command name for this rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>command_name must be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• abor: Abort command</td>
</tr>
<tr>
<td>• cwd: Current working directory command</td>
</tr>
<tr>
<td>• eprt: eprt command</td>
</tr>
<tr>
<td>• epsv: epsv command</td>
</tr>
<tr>
<td>• list: List command</td>
</tr>
<tr>
<td>• mode: Transfer mode command</td>
</tr>
<tr>
<td>• pass: Password command</td>
</tr>
<tr>
<td>• pasv: Passive command</td>
</tr>
<tr>
<td>• port: Port command</td>
</tr>
<tr>
<td>• quit: Quit command</td>
</tr>
<tr>
<td>• rest: Restore command</td>
</tr>
<tr>
<td>• retr: Retry command</td>
</tr>
<tr>
<td>• stor: Store command</td>
</tr>
<tr>
<td>• stru: file structure command</td>
</tr>
<tr>
<td>• syst: system command</td>
</tr>
<tr>
<td>• type: Type command</td>
</tr>
<tr>
<td>• user: user command</td>
</tr>
</tbody>
</table>
Usage

Use this command to specify a rule definition to analyze user traffic based on an FTP command name.

Example

The following command creates an FTP rule definition for analyzing user traffic using the FTP command name of *list*:

```shell
ftp command name = list
```
ftp connection-type

This command defines a rule definition to analyze and charge user traffic based on FTP connection type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] ftp connection-type operator connection_type
```

- `no`
  - Removes the specified rule definition.

- `operator`
  - Specifies how to logically match the information in the analyzed field.
  - `operator` must be one of the following:
    - `!=`: does not equal
    - `<=`: less than or equals
    - `==`: equals
    - `>=`: greater than or equals

- `connection_type`
  - Specifies the connection type for this rule definition.
  - `connection_type` must be one of the following:
    - `0`: unknown
    - `1`: control connection
    - `2`: data connection

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an FTP connection type.

**Example**

The following command creates an FTP rule definition for analyzing user traffic using an FTP connection type of 1:

```plaintext
ftp connection-type = 1
```
ftp data-any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for FTP data packets.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
[ no ] ftp data-any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  - `operator` must be one of the following:
    - `! =`: does not equal
    - `= =`: equals

- **condition**
  Specifies the condition for this rule definition.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the any match status for FTP data packets.

**Example**
The following command creates a rule definition for analyzing user traffic using data-any-match status for FTP data packet set as `FALSE`:

```bash
ftp data-any-match = FALSE
```
ftp filename

This command defines a rule definition to analyze and charge user traffic based on FTP file name.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp filename [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• !contains: does not contain
• !ends-with: does not end with
• !starts-with: does not start with
• =: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

string
Specifies the string for this rule definition. string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on an FTP filename.

Example
The following command creates an FTP rule definition for analyzing user traffic using an FTP filename of test:

ftp filename = test
ftp pdu-length

This command defines a rule definition to analyze and charge user traffic based on FTP Protocol Data Unit (PDU) length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp pdu-length operator pdu_length

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

• !=: does not equal
• <=: less than or equals
• ==: equals
• >=: greater than or equals

pdu_length
Specifies the FTP PDU length, in bytes, for this rule definition.
pdu_length must be an integer from 0 through 65535.

Usage
Use this command to specify a rule definition to analyze user traffic based on FTP PDU length (header + payload) in bytes.

Example
The following command creates an FTP rule definition for analyzing user traffic using an FTP pdu length of 9647 bytes:

ftp pdu-length = 9647
ftp pdu-type

This command defines a rule definition to analyze and charge user traffic based on FTP Protocol Data Unit (PDU) type.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp pdu-type operator pdu_type

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

• !: does not equal
• <=: less than or equals
• =: equals
• =>: greater than or equals

pdu_type
Specifies the PDU type for this rule definition.
pdu_type must be one of the following:

• 0: unknown
• 1: command
• 2: reply

Usage
Use this command to specify a rule definition to analyze user traffic based on an FTP PDU type.

Example
The following command creates an FTP rule definition for analyzing user traffic using an FTP PDU type of 0:

ftp pdu-type = 0
ftp previous-state

This command defines a rule definition to analyze and charge user traffic based on the previous state of FTP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp previous-state operator previous_state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • !=: does not equal
  • ==: equals

previous_state
Specifies the previous state.
previous_state must be one of the following:
  • command-sent
  • init
  • response-error
  • response-ok

Usage
Use this command to specify a rule definition to analyze user traffic based on a previous state.

Example
The following command creates an FTP rule definition for analyzing user traffic using a previous FTP state of init:

ftp previous-state = init
ftp reply code

This command defines a rule definition to analyze and charge user traffic based on the FTP reply code.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ftp reply code operator code
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **code**
  Specifies the code for this rule definition.
  `code` must be an integer from 100 through 599.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an FTP reply.

**Example**
The following command creates an FTP rule definition for analyzing user traffic using an FTP reply code of 199:

```
ftp reply code = 199
```
ftp server-ip-address

This command defines a rule definition to analyze and charge user traffic based on the FTP server IP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp server-ip-address operator ip_address

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>must be one of the following:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>! =</th>
</tr>
</thead>
<tbody>
<tr>
<td>does not equal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;=</th>
</tr>
</thead>
<tbody>
<tr>
<td>less than or equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>=</th>
</tr>
</thead>
<tbody>
<tr>
<td>equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&gt;=</th>
</tr>
</thead>
<tbody>
<tr>
<td>greater than or equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the server address for this rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>must be expressed in IPv4 decimal notation or IPv6 colon notation.</td>
</tr>
</tbody>
</table>

Usage

Use this command to specify a rule definition to analyze user traffic based on an FTP server IP address.

Example

The following command creates an FTP rule definition for analyzing user traffic using an FTP server IP of 1.1.1.1:

```
ftp server-ip-address = 1.1.1.1
```
ftp server-port

This command defines a rule definition to analyze and charge user traffic based on the FTP server port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] ftp server-port operator port
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• ! =: does not equal</td>
</tr>
<tr>
<td>• &lt;=: less than or equals</td>
</tr>
<tr>
<td>• =: equals</td>
</tr>
<tr>
<td>• &gt;=: greater than or equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the FTP server port.</td>
</tr>
<tr>
<td>port must be an integer from 1 through 65535.</td>
</tr>
</tbody>
</table>

Usage
Use this command to specify a rule definition to analyze user traffic based on an FTP server port.

Example
The following command creates an FTP rule definition for analyzing user traffic using ftp server port 25:

```
ftp server-port = 25
```
ftp session-length

This command defines a rule definition to analyze and charge user traffic based on the FTP session-length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp session-length operator session_length

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• < <=: less than or equals
• =: equals
• >=: greater than or equals

session_length
Specifies the FTP session length for this rule definition.
session_length must be an integer from 1 through 4000000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on the FTP session’s total length.

Example
The following command creates a rule definition for analyzing user traffic using an FTP session length of 40000:

ftp session-length = 40000
ftp state

This command defines a rule definition to analyze and charge user traffic based on the FTP state.

Product
All

Privilege
Security Administrator, Administrator

Syntax
[
  no
] ftp state operator { close | command-sent | init | response-error | response-ok }

  no
  Removes the specified rule definition.

  operator
  Specifies how to logically match the information in the analyzed field. 
  operator must be one of the following:
  • !=: does not equal
  • ==: equals

  close
  Analyzes FTP transmissions that are in a closed state.

  command-sent
  Analyzes FTP transmissions that are in a command sent state.

  init
  Analyzes FTP transmissions that are in the initialized state.

  response-error
  Analyzes FTP transmissions that are in the response error state.

  response-ok
  Analyzes FTP transmissions that are in the response ok state.

Usage
Use this command to specify a rule definition to analyze user traffic based on the current ftp session state.

Example
The following command creates an FTP rule definition for analyzing user traffic using a current FTP state of open:

[ no ] ftp state operator { close | command-sent | init | response-error | response-ok }
ftp state = open
ftp url

This command defines a rule definition to analyze and charge user traffic based on the FTP URL.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp url [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

• !=: does not equal
• !=contains: does not contain
• !=ends-with: does not end with
• !=starts-with: does not start with
• =: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

string
A unique name that you specify for the FTP URL.
string must be an alpha and/or numeric string of 1 through 127 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on FTP file location/path for transfer.

Example
The following command creates an FTP rule definition for analyzing user traffic using an FTP URL string of ftp://rfc.ietf.org/rfc/rfc1738.txt:
ftp url = ftp://rfc.ietf.org/rfc/rfc1738.txt
ftp user

This command defines a rule definition to analyze and charge user traffic based on the FTP user.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ftp user [ case-sensitive ] operator ftp_user

- no
  Removes the specified rule definition.

- case-sensitive
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- operator
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  • !=: does not equal
  • !=contains: does not contain
  • !=ends-with: does not end with
  • !=starts-with: does not start with
  • =: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

- ftp_user
  A unique name that you specify for the FTP user. ftp_user must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on the FTP user.

Example
The following command creates an FTP rule definition for analyzing user traffic using an FTP user of user1:

```
ftp user = user1
```
The following commands define rule for analyzing traffic based on Hypertext Transport Protocol (HTTP):
# http attribute-in-data

This command enables configuring dynamic header field in application payload.

## Product

All

## Privilege

Security Administrator, Administrator

## Syntax

```
[ no ] http attribute-in-data field_name [ case-sensitive ] operator string
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the specified rule definition.</td>
</tr>
<tr>
<td>case-sensitive</td>
<td>This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive. Default: Disabled</td>
</tr>
<tr>
<td>operator</td>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
<tr>
<td>field_name</td>
<td>Specifies the name of the field. field_name must be an alpha and/or numeric string of 1 through 31 characters in length.</td>
</tr>
<tr>
<td>string</td>
<td>Specifies value of the extension header. field_name must be an alpha and/or numeric string of 1 through 127 characters in length.</td>
</tr>
</tbody>
</table>

## Usage

Use this command to configure dynamic header field in application payload.
http attribute-in-url

This command enables configuring dynamic header field in URL.

Product  
All

Privilege  
Security Administrator, Administrator

Syntax

[ no ] http attribute-in-url field_name [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive. 
Default: Disabled

operator
Specifies how to logically match the information in the analyzed field. 
operator must be one of the following:
  • !=: does not equal
  • !contains: does not contain
  • !ends-with: does not end with
  • !starts-with: does not start with
  • =: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

field_name
Specifies the name of the field.  
field_name must be an alpha and/or numeric string of 1 through 31 characters in length.

string
Specifies value of the extension header.  
field_name must be an alpha and/or numeric string of 1 through 127 characters in length.

Usage

Use this command to configure dynamic header field in URL.
http any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for HTTP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http any-match [operator condition]
```

- `no`
  Removes the specified rule definition.

- `operator`
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `! =`: does not equal
  - `=`: equals

- `condition`
  Specifies the condition for this rule definition. `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the HTTP any match status.

**Example**

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP any match status of FALSE:

```
http any-match = FALSE
```
http content disposition

This command defines a rule definition to analyze and charge user traffic based on the optional “content disposition” field of HTTP entity header.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http content disposition [ case-sensitive ] operator content_dispos
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - !=: does not equal
  - !contains: does not contain
  - !ends-with: does not end with
  - !starts-with: does not start with
  - ==: equals
  - contains: contains
  - ends-with: ends with
  - starts-with: starts with

- **content_dispos**
  This field offers a mechanism for the sender to transmit presentational information to the recipient, allowing each component of a message to be tagged with an indication of its desired presentation semantics.
  **content_dispos** must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an HTTP content type. This feature is to support RFC 2616 for HTTP and RFC 1806 for Content Disposition.
Example
The following command creates an HTTP rule definition for analyzing user traffic using content-disposition field in an HTTP entity header as *successful*:

```
http content disposition = successful
```
http content length

This command defines a rule definition to analyze and charge user traffic based on HTTP content length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http content length operator content_length

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `=>`: greater than or equals

- **content_length**
  Specifies the HTTP body length, in bytes, for this rule definition.
  `content_length` must be an integer from 1 through 4000000000.

Usage

Use this command to specify a rule definition to analyze user traffic based on an HTTP content length.

Example

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP body length of 10000:

```
http content length = 10000
```
http content type

This command defines a rule definition to analyze and charge user traffic on the basis of content-type field in HTTP entity header.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http content type [ case-sensitive ] operator content_type

no
Removes the specified rule definition.

case-sensitive
Default: Disabled
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
• !=: does not equal
• !contains: does not contain
• !ends-with: does not end with
• !starts-with: does not start with
• ==: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

content_type
A unique content type that you specify for the HTTP rule definition. content_type must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on content-type field in HTTP entity header.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP content type of "abc100."

```
http content type = abc100
```
http error

This command defines a rule definition to analyze user traffic for invalid HTTP packets and other errors while parsing HTTP packets.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http error operator condition

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>*!=: does not equal</td>
</tr>
<tr>
<td>*=: equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the condition for this rule definition.</td>
</tr>
<tr>
<td>condition must be one of the following:</td>
</tr>
<tr>
<td>*FALSE</td>
</tr>
<tr>
<td>*TRUE</td>
</tr>
</tbody>
</table>

Usage

Use this command to define a rule definition to analyze user traffic for invalid HTTP packets and any other errors while parsing HTTP packets. For example, FSM error, invalid header field values, ACS memory and buffer limit, packet related errors.

ECS supports pipelining of up to 32 HTTP requests on the same TCP connection. Pipeline overflow requests are not analyzed. Such overflow requests are treated as http-error. The billing system, based on this information, decides to charge or not charge, or refund the subscriber accordingly.

Example

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP error status of TRUE:

```
http error = TRUE
```
http first-request-packet

This command defines a rule definition to analyze and charge user traffic based on the HTTP first-requestACKET.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] http first-request-packet operator condition
```

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - `operator` must be one of the following:
    - `!=`: does not equal
    - `==`: equals

- **condition**
  - Specifies the condition for this rule definition.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the HTTP first request packet.

**Example**

The following command creates an HTTP rule definition for analyzing user traffic testing for the first-request-packet equals `TRUE`:

```
http first-request-packet = TRUE
```
http header-length

This command defines a rule definition to analyze and charge user traffic based on HTTP header length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http header-length operator header_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than or equals
  - `=`: equals
  - `>`: greater than or equals

- **header_length**
  Specifies the HTTP header length, in bytes, for this rule definition. `header_length` must be an integer from 0 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on HTTP header length.

**Example**
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP header length of 10000:

```
http header-length = 10000
```
http host

This command defines a rule definition to analyze and charge user traffic based on HTTP host.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http host [ case-sensitive ] operator host_name
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **host_name**
  A unique name that you specify for the HTTP host.
  *host_name* must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an HTTP host name.

**Example**

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP host of `host1`:

```
http host host1
```
http host = host1
**http payload-length**

This command defines a rule definition to analyze and charge user traffic based on HTTP payload length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http payload-length operator payload_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `>=`: greater than or equals

- **payload_length**
  Specifies the HTTP payload (content) length, in bytes, for this rule definition.
  `payload_length` must be an integer from 1 through 400000000.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an HTTP payload length.

**Example**

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP payload length of 10000 bytes:

```
http payload-length = 10000
```
http pdu-length

This command defines a rule definition to analyze and charge user traffic based on HTTP Protocol Data Unit (PDU) length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http pdu-length operator pdu_length

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- \(!=\): does not equal
- \(<\leq\): less than or equals
- \(\leq\): equals
- \(>\leq\): greater than or equals

pdu_length
Specifies the HTTP PDU length, in bytes, for this rule definition. pdu_length must be an integer from 0 through 65535.

Usage
Use this command to specify a rule definition to analyze user traffic based on an HTTP PDU length (header + payload) in bytes.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP PDU length of 10000 bytes:

http pdu-length = 10000
http previous-state

This command defines a rule definition to analyze and charge user traffic based on HTTP previous state.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http previous-state operator previous_state

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **previous_state**
  Specifies the HTTP previous state for this rule definition.
  previous_state must be one of the following:
  - `init`: init state
  - `response-error`: response error state
  - `response-ok`: response ok state
  - `waiting-for-response`: waiting for response state

Usage
Use this command to specify a rule definition to analyze user traffic based on an HTTP previous state.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP previous state of `response-ok`:

```
http previous-state = response-ok
```
http referer

This command defines a rule definition to analyze and charge user traffic based on HTTP referer link.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] http referer [ case-sensitive ] operator referer_name
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **referer_name**
  A unique name that you specify for the HTTP referer.
  *referer_name* must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on an HTTP referer name. This feature provides the ability to operator to ECS collect or track all URLs visited during a particular subscriber session. These URLs would include the entire string of visited URLs including all referral links. This information output is used in an EDR format to use for reporting or billing functions.

For example, if subscriber begins a web session on his phone and click on the “Sports” link from his home deck and then choose ESPN and from ESPN move to an advertiser link, operator can capture all URLs for
that entire session, and during this period ECS collects the URLs for a particular subscriber session and be limited to time duration or number of URLs visited. ECS supports EDRs for this and EDRs generated contains HTTP URL and the HTTP referer fields along with other fields.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP referer to cricket.espn.com

```plaintext
http referer = cricket.espn.com
```
http reply code

This command defines a rule definition to analyze and charge user traffic based on HTTP reply.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http reply code operator reply_code

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- <=: less than or equals
- ==: equals
- >=: greater than or equals

reply_code
Specifies the HTTP response for this rule definition. reply_code must be an integer from 100 through 599.

Usage
Use this command to specify a rule definition to analyze user traffic based on an HTTP reply code.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP reply code of 356:

http reply code = 356
http request method

This command defines a rule definition to analyze and charge user traffic based on HTTP request method.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] http request method operator request
```

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - **operator** must be one of the following:
    - `!=`: does not equal
    - `=`: equals

- **request**
  - Specifies the HTTP request for this rule definition.
  - **request** must be one of the following requests:
    - `connect`
    - `delete`
    - `get`
    - `head`
    - `options`
    - `post`
    - `put`
    - `trace`

Usage

Use this command to specify a rule definition to analyze user traffic based on HTTP request method.

Example

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP request method of `connect`:

```plaintext
http request method = connect
```
http session-length

This command defines a rule definition to analyze and charge user traffic based on HTTP session length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http session-length operator session_length

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- <=: less than or equals
- ==: equals
- >=: greater than or equals

session_length
Specifies the HTTP total session length for this rule definition. session_length must be an integer from 1 through 4000000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on the total HTTP session length.

Example
The following command creates an HTTP rule definition for analyzing user traffic using a total HTTP session length of 200000:

http session-length = 200000
http state

This command defines a rule definition to analyze and charge user traffic based on HTTP state.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http state operator state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• ==: equals

state
Specifies the HTTP state for this rule definition.
state must be one of the following:
• close: closed state
• response-error: response error state
• response-ok: response ok state
• waiting-for-response: waiting for response state

Usage
Use this command to specify a rule definition to analyze user traffic based on an HTTP state.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP state of init:

    http state = init
http transaction-length

This command defines a rule definition to analyze and charge user traffic based on HTTP transaction length (combined length of one HTTP GET Request message and associated one or more response message).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http transaction-length { operator trans_length | { range | !range
range_from to range_to } }
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than or equals
  - `=`: equals
  - `>`: greater than or equals

- **trans_length**
  Specifies the HTTP transaction length, in bytes, for this rule definition.
  `trans_length` must be an integer from 1 through 400000000.

- **range**
  Enables or disables the range criteria for length of transaction.
  `range`: Enables the range criteria for HTTP transaction length.
  `!range`: Disables the range criteria for HTTP transaction length.

- **range_from**
  Specifies the start of range, in bytes, for HTTP transaction length.

- **range_to**
  Specifies the end of range, in bytes, for HTTP transaction length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on HTTP transaction length (one HTTP GET Request message + one or more associated response message/s) in bytes.

**Example**

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP transaction length of 10200 bytes:

```
http transaction-length = 10200
http transfer-encoding

This command defines a rule definition to analyze and charge user traffic based on HTTP encoding.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] http transfer-encoding [ case-sensitive ] operator string
```

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
opeator must be one of the following:

- `!`: does not equal
- `!contains`: does not contain
- `!ends-with`: does not end with
- `!starts-with`: does not start with
- `=`: equals
- `contains`: contains
- `ends-with`: ends with
- `starts-with`: starts with

string
A unique name that you specify for HTTP transfer encoding.
string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on an HTTP transfer encoding string.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP transfer encoding string of user1:

```
http transfer-encoding = user1
```
http uri

This command defines a rule definition to analyze and charge user traffic based on HTTP uniform resource identifier (URI).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http uri [ case-sensitive ] operator string

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Removes the specified rule definition.

<table>
<thead>
<tr>
<th>case-sensitive</th>
</tr>
</thead>
</table>
| Default: Disabled. This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
</table>
| Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- !=contains: does not contain
- !=ends-with: does not end with
- !=starts-with: does not start with
- =: equals
- contains: contains
- ends-with: ends with
- starts-with: starts with

<table>
<thead>
<tr>
<th>string</th>
</tr>
</thead>
</table>
| A unique name that you specify for the HTTP URI. string must be an alpha and/or numeric string of 1 through 127 characters in length. string allows punctuation characters and it does not include the “host” portion.

Usage
Use this command to specify a rule definition to analyze user traffic based on an HTTP URI.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP URI string of http://www.somehost.com:

```
http uri = http://www.somehost.com
```
http url

This command defines a rule definition to analyze and charge user traffic based on HTTP URL.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http url [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

• !=: does not equal
• !contains: does not contain
• !ends-with: does not end with
• !starts-with: does not start with
• =: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

string
A unique name that you specify for the HTTP URL.
string must be an alpha and/or numeric string of 1 through 127 characters in length. string allows punctuation characters and includes “host + URI” for HTTP PDUs.
For example, in case of the URL “http://www.google.fr”, the host is “http://www.google.fr”, and the URI is “/”: 

Hypertext Transfer Protocol GET / HTTP/1.1\nRequest Method: GET
Request URI: / Request Version: HTTP/1.1 Accept: */*
Accept-Language: fr
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.google.fr
**Usage**

Use this command to specify a rule definition to analyze user traffic based on an HTTP URL.

**Example**

The following command creates an HTTP rule definition for analyzing user traffic using an HTTP URL string of http://rfc.ietf.org/rfc/rfc1738.txt:

```
http url = http://rfc.ietf.org/rfc/rfc1738.txt
```
**http user-agent**

This command defines a rule definition to analyze and charge user traffic based on the user agent information in “user-agent” field of HTTP header.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http user-agent [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!=contains`: does not contain
  - `!=ends-with`: does not end with
  - `!=starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  This matches the HTTP user agent information in HTTP header.
  `string` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the HTTP “user-agent” field.

**Example**
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP user agent as *xyz.123*:

```
http user-agent = xyz.123
```
http version

This command defines a rule definition to analyze and charge user traffic based on HTTP version information in header.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] http version [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• ! =: does not equal
  • ! contains: does not contain
  • ! ends-with: does not end with
  • ! starts-with: does not start with
  • =: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

string
This matches the HTTP version information in HTTP header.
string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on the HTTP version.

Example
The following command creates an HTTP rule definition for analyzing user traffic using an HTTP version of http/2:

http version
http version = http4.2
**http x-header**

This command configures and matches rules based on extension-headers (x-headers). All x-header fields must begin with “x-.”

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] http x-header name [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **name**
  A unique value that you specify to use for the x-header.
  `name` must be an alpha and/or numeric string of 1 through 31 characters in length.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  This matches the HTTP x-header information in HTTP header.
  `string` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**
Use this command to configure and match rules based on extension-headers (x-headers). This allows additional header fields to be defined without changing the protocol. The extension-header can be any header fields which are not specified in RFC.

**Example**
The following command creates a rule definition for analyzing user traffic containing extension-header of *test_field* and value of *test_string*:

```
http x-header test_field = test_string
```

icmp

The following commands define rules for analyzing traffic based on Internet Control Message Protocol (ICMP):
icmp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for ICMP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] icmp any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `! =`: does not equal
  - `= :`: equals

- **condition**
  Specifies the condition for this rule definition. 
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the icmp analyzed state.

**Example**

The following command creates a icmp rule definition for analyzing user traffic using an ICMP any match state of `FALSE`.

```
icmp any-match = FALSE
```
icmp code

This command defines a rule definition to analyze and charge user traffic based on the ICMP code.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] icmp code operator code
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than or equals
  - `=`: equals
  - `>`: greater than or equals

- **code**
  Specifies the ICMP code is for this rule definition. `code` must be an integer from 0 through 255.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the ICMP code.

**Example**

The following command creates an ICMP rule definition for analyzing user traffic using an ICMP code as 23:

```
icmp code = 23
```
icmp type

This command defines a rule definition to analyze and charge user traffic based on the ICMP type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] icmp type operator type
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than or equals
  - `=`: equals
  - `>`: greater than or equals

- **type**
  Specifies the ICMP type for this rule definition.
  `type` must be an integer from 0 through 255. For example, 0 for ECHO Reply, 3 for Destination Unreachable, and 5 for Redirect.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the ICMP type.

**Example**

The following command creates an ICMP rule definition for analyzing user traffic using an ICMP type as 123:

```
icmp type = 123
```
icmpv6

The following commands define rules for analyzing traffic based on Internet Control Message Protocol Version 6 (ICMPv6).
icmpv6 any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for Internet Control Message Protocol Version 6 (ICMPv6).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] icmpv6 any-match operator condition

- no
  Removes the specified rule definition.

- operator
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  • ! =: does not equal
  • =: equals

- condition
  Specifies the condition for this rule definition.
  condition must be one of the following:
  • FALSE
  • TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the ICMPv6 analyzed state.

Example
The following command creates an ICMPv6 rule definition for analyzing user traffic using an ICMPv6 any match state of FALSE:

    icmpv6 any-match = FALSE
**icmpv6 code**

This command defines a rule definition to analyze and charge user traffic based on the ICMPv6 code.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] icmpv6 code operator code
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **code**
  Specifies the ICMPv6 code is for this rule definition.
  `code` must be an integer from 0 through 255.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the ICMPv6 code.

**Example**

The following command creates an ICMPv6 rule definition for analyzing user traffic using an ICMPv6 code as 23:

```
icmpv6 code = 23
```
icmpv6 type

This command defines a rule definition to analyze and charge user traffic based on the ICMPv6 type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] icmpv6 type operator type
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  - `!` or `!=`: does not equal
  - `<` or `<=`: less than or equals
  - `=`: equals
  - `>` or `>=`: greater than or equals

- **type**
  Specifies the ICMPv6 type for this rule definition.
  `type` must be an integer from 0 through 255. For example, 0 for ECHO Reply, 3 for Destination Unreachable, and 5 for Redirect.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the ICMPv6 type.

**Example**
The following command creates an ICMPv6 rule definition for analyzing user traffic using an ICMPv6 type as 123:

```
icmpv6 type = 123
```
if-protocol

This command allows different content IDs with certain protocols to be associated with the same.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
if-protocol [ http | wsp-connection-less | wsp-connection-oriented ] content-id content_id
```

```
no if-protocol [ http | wsp-connection-less | wsp-connection-oriented ]
```

**no**

Removes the specified rule definition.

**http**

Specifies HTTP protocol for the rule definition.

**wsp-connection-less**

This routes the packets to WSP connection less protocol.

**wsp-connection-oriented**

This routes the packets to WSP connection oriented protocol.

**content-id content_id**

Specifies content ID used to give to the rule definition.

`content_id` must be an integer from 1 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on if-protocol.

**Example**

The following command creates an if-protocol rule definition for analyzing user traffic using http and a content ID of 23:

```
if-protocol http content-id 23
```
The following commands define rules for analyzing traffic based on Internet Message Access Protocol (IMAP):
imap any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for IMAP message packets.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] imap any-match operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

• !=: does not equal
• =: equals

condition
Specifies the condition for this rule definition. condition must be one of the following:

• FALSE
• TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the any-match analyzed state.

Example
The following command creates IMAP rule definition for analyzing user traffic using an IMAP any match state of FALSE:

imap any-match = FALSE
imap cc

This command defines a rule definition to analyze and charge user traffic based on the recipient address in the Carbon Copy (cc) field of e-mail in the IMAP message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imap cc [ case-sensitive ] operator cc_address
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  The `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **cc_address**
  Specifies the string for this rule definition.
  The `cc_address` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the recipient address in the “cc” field of e-mail in the IMAP message of analyzed state.

**Example**
The following command creates IMAP rule definition for analyzing user traffic using recipient address `triangular@xyz.com` in the “cc” field of e-mail in the IMAP message:

```
imap cc contains triangular@xyz.com
```
imap command

This command defines a rule definition to analyze and charge user traffic based on the embedded IMAP commands in the IMAP message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] imap command operator commands
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `! =`: does not equal
  - `=`: equals

- **commands**
  Specifies the command for this rule definition.
  `commands` must be one of the following:
  - `append`
  - `authenticate`
  - `capability`
  - `check`
  - `close`
  - `copy`
  - `create`
  - `delete`
  - `examine`
  - `expunge`
  - `fetch`
  - `list`
  - `login`
  - `logout`
  - `lsUB`
  - `noop`
imap command

• rename
• search
• select
• starttls
• status
• store
• subscribe
• uid-copy
• uid-fetch
• uid-search
• uid-store
• unsubscribe

Usage
Use this command to specify a rule definition to analyze user traffic based on the embedded command in the IMAP message of analyzed state.

Example
The following command creates IMAP rule definition for analyzing user traffic using presence of close command in the IMAP message;

imap command = close
imap content class

This command defines a rule definition to analyze and charge user traffic based on the “content-class” field of e-mail in the IMAP message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] imap content class [ case-sensitive ] operator content_class

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - • !=: does not equal
  - • !contains: does not contain
  - • !ends-with: does not end with
  - • !starts-with: does not start with
  - • =: equals
  - • contains: contains
  - • ends-with: ends with
  - • starts-with: starts with

- **content_class**
  Specifies the string for this rule definition.
  **content_class** must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on the “content-class” field of e-mail in the IMAP message of analyzed state.

Example
The following command creates IMAP rule definition for analyzing user traffic using content class as `javax.mail.internet.MimeMultipart` in the "content-class" field of e-mail in the IMAP message:

```
imap content class contains javax.mail.internet.MimeMultipart
```
imap content type

This command defines a rule definition to analyze and charge user traffic based on the “content-type” field of e-mail in the IMAP message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] imap content type [ case-sensitive ] operator content_type

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !=: does not equal
- !contains: does not contain
- !ends-with: does not end with
- !starts-with: does not start with
- =: equals
- contains: contains
- ends-with: ends with
- starts-with: starts with

content_type
Specifies the string for this rule definition.
content_type must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on the “content-type” field of e-mail in the IMAP message of analyzed state.

Example
The following command creates IMAP rule definition for analyzing user traffic using content type `TEXT/plain; charset=iso-8859-1` in the 'content-type' field of e-mail in the IMAP message:

```
imap content type contains TEXT/plain; charset=iso-8859-1
```
**imap date**

This command defines a rule definition to analyze and charge user traffic based on the “date” field of e-mail in the IMAP message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imap date [ case-sensitive ] operator date
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **date**
  Specifies the string for this rule definition.
  `date` must be an alpha and/or numeric string of 1 through 127 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the “date” field of e-mail in the IMAP message of analyzed state.

**Example**
The following command creates IMAP rule definition for analyzing user traffic using date Fri, 21 Nov 1997 11:00:00 -0600 in the “date” field of e-mail in the IMAP message:

```
imap date contains Fri, 21 Nov 1997 11:00:00 -0600
```
imap final-reply

This command defines a rule definition to analyze and charge user traffic based on the “final-reply” value of the last IMAP final-reply message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] imap final-reply operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
  • !=: does not equal
  • ==: equals

condition
Specifies the ‘final-reply’ condition value for the last IMAP final-reply message to match the information in the analyzed field. condition must be one of the following:
  • bad: final reply is invalid or bad.
  • no: there is no final reply.
  • ok: final reply is valid.

Usage
Use this command to specify a rule definition to analyze user traffic based on using the final-reply value of the last IMAP final-reply message of analyzed state.

Example
The following command creates IMAP rule definition for analyzing user traffic using the final-reply condition value as bad for the last IMAP final-reply message:

imap final-reply = bad
**imap from**

This command defines a rule definition to analyze and charge user traffic based on the “from” field of e-mail in the IMAP message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imap from [ case-sensitive ] operator from_string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `< ! = >`: does not equal
  - `< ! contains >`: does not contain
  - `< ! ends-with >`: does not end with
  - `< ! starts-with >`: does not start with
  - `< = >`: equals
  - `< contains >`: contains
  - `< ends-with >`: ends with
  - `< starts-with >`: starts with

- **from_string**
  Specifies the string for this rule definition.
  `from_string` must be an alpha and/or numeric string of 1 through 127 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the “from” field of e-mail in the IMAP message of analyzed state.
The following command creates IMAP rule definition for analyzing user traffic using occurrence of triangular in the “from” field of e-mail in the IMAP message:

```
imap from contains triangular
```
imap mail-size

This command defines a rule definition to analyze and charge user traffic based on the size of e-mail in retrieved by IMAP from server.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] imap mail-size operator mail_size

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

• !=: does not equal
• <:= less than or equals
• :=: equals
• >=: greater than or equals

mail_size
Specifies the total size of mail in bytes retrieved by IMAP from server for this rule definition. mail_size must be an integer from 0 through 4000000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on the size of e-mail in the IMAP message of analyzed state. This rule uses size of the given mail retrieved by IMAP from server.

Example
The following command creates IMAP rule definition for analyzing user traffic using size of e-mail as less than or equal to 23400 bytes in the IMAP message:

imap mail-size <= 23400
imap mailbox-size

This command defines a rule definition to analyze and charge user traffic based on the number of e-mail messages in a mailbox of an IMAP e-mail user.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] imap mailbox-size operator mail_qty

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !: does not equal
- <: less than or equals
- =: equals
- =>: greater than or equals

mail_qty
Specifies the total number of e-mail messages in a mailbox of the IMAP user for this rule definition.
mail_qty must be an integer from 0 through 65535.

Usage
Use this command to specify a rule definition to analyze user traffic based on the size of mailbox of an IMAP message user of analyzed state. This rule uses number of E-mails messages contained in a mailbox.

Example
The following command creates IMAP rule definition for analyzing user traffic using number of e-mail messages in a mailbox to less than or equal to 1024:

imap mailbox-size <= 1024
imap message-type

This command defines a rule definition to analyze and charge user traffic based on the type of message in IMAP packet header.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
[ no ] imap message-type operator type
```

<table>
<thead>
<tr>
<th>no</th>
<th>Removes the specified rule definition.</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>Specifies how to logically match the information in the analyzed field. operator must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• !=: does not equal</td>
</tr>
<tr>
<td></td>
<td>• ==: equals</td>
</tr>
<tr>
<td>condition</td>
<td>Specifies the message-type condition/value for the IMAP e-mail message to match the information in the analyzed field. condition must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• command-continuation-reply: message with command-continuation-reply type.</td>
</tr>
<tr>
<td></td>
<td>• final-reply: message is of final reply type.</td>
</tr>
<tr>
<td></td>
<td>• request: there is of request type.</td>
</tr>
<tr>
<td></td>
<td>• untagged-reply: message of reply type, but without any tag.</td>
</tr>
</tbody>
</table>

Usage
Use this command to specify a rule definition to analyze user traffic based on using the type of message in “message-type” filed of the last IMAP message of analyzed state.

Example
The following command creates IMAP rule definition for analyzing user traffic using the message type as request for the IMAP message:

```bash
imap message-type = request
```
**imap previous-state**

This command defines a rule definition to analyze and charge user traffic based on the previous state of IMAP message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imap previous-state operator state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **state**
  Specifies the previous state of the IMAP message to match the information in the analyzed field.
  *state* must be one of the following:
  - `init`: message in initialization state.
  - `request-sent`: message in request-sent state.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on using the previous state of the IMAP message of analyzed state.

**Example**

The following command creates IMAP rule definition for analyzing user traffic using the previous state as *init* of the IMAP message which was in initialization state:

```
imap previous-state = init
```
imap session-length

This command defines a rule definition to analyze and charge user traffic based on the IMAP session length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imap session-length operator session_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **session_length**
  Specifies the total length of IMAP session, in bytes, for this rule definition.
  `session_length` must be an integer from 1 through 4000000000.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the length of IMAP session of the analyzed state.
The session length is calculated by adding together the IP payloads (i.e., starting after the IP header) of all relevant IMAP session packets.

**Example**
The following command creates IMAP rule definition for analyzing user traffic using session length as less than or equal to 4000 bytes for the IMAP session:

```
imap session-length <= 4000
```
imap session-previous-state

This command defines a rule definition to analyze and charge user traffic based on the previous state of IMAP session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imap session-previous-state operator state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. **operator** must be one of the following:
  - `!`: does not equal
  - `=`: equals

- **state**
  Specifies the previous state of the IMAP session to match the information in the analyzed field. **state** must be one of the following:
  - `authenticated`: session authenticated
  - `connected`: session connected
  - `init`: session initialized
  - `mailbox-selected`: mailbox selected

**Usage**

Use this command to specify a rule definition to analyze user traffic based on using the previous state of the IMAP session of analyzed state.

**Example**

The following command creates IMAP rule definition for analyzing user traffic using the previous state as `init` of the IMAP session which was initialized:

```
imap session-previous-state = init
```
imap session-state

This command defines a rule definition to analyze and charge user traffic based on the current state of IMAP session.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] imap session-state operator state
```

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the specified rule definition.</td>
</tr>
<tr>
<td>operator</td>
<td>Specifies how to logically match the information in the analyzed field. operator must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• !=: does not equal</td>
</tr>
<tr>
<td></td>
<td>• ==: equals</td>
</tr>
<tr>
<td>state</td>
<td>Specifies the current state of the IMAP session to match the information in the analyzed field. state must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• authenticated: session authenticating.</td>
</tr>
<tr>
<td></td>
<td>• connected: session connecting.</td>
</tr>
<tr>
<td></td>
<td>• logout: session logged out.</td>
</tr>
<tr>
<td></td>
<td>• mailbox-selected: mailbox selecting.</td>
</tr>
</tbody>
</table>

Usage

Use this command to specify a rule definition to analyze user traffic based on using the current state of the IMAP session of analyzed state.

Example

The following command creates IMAP rule definition for analyzing user traffic using the current state as connected of the IMAP session which is in connecting state:

```
imap session-state = connected
```
**imap state**

This command defines a rule definition to analyze and charge user traffic based on the current state of IMAP request message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imap state operator state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `! =`: does not equal
  - `= =`: equals

- **state**
  Specifies the current state of the IMAP request message to match the information in the analyzed field.
  *state* must be one of the following:
  - `request-sent`: request message sent
  - `response-fail`: request response failed
  - `response-ok`: request response is good

**Usage**

Use this command to specify a rule definition to analyze user traffic based on using the current state of the IMAP request message of analyzed state.

**Example**

The following command creates IMAP rule definition for analyzing user traffic using the current state as `response-fail` of the IMAP request message when request response is failed:

```
imap state = response-fail
```
imap subject

This command defines a rule definition to analyze and charge user traffic based on the ‘subject’ field of e-mail in the IMAP message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] imap subject [ case-sensitive ]operatorsubject

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - !:= does not equal
  - !contains: does not contain
  - !ends-with: does not end with
  - !starts-with: does not start with
  - := equals
  - contains: contains
  - ends-with: ends with
  - starts-with: starts with

- **subject**
  Specifies the string for this rule definition.
  **subject** must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on the “subject” field of e-mail in the IMAP message of analyzed state.

Example
The following command creates IMAP rule definition for analyzing user traffic using occurrence of *My test* in the “subject” field of e-mail in the IMAP message:

```
imap subject contains My test
```
imap to

This command defines a rule definition to analyze and charge user traffic based on the ‘to’ field of e-mail in the IMAP message.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] imap to [ case-sensitive ] operatorsubject
```

- **no**
  - Removes the specified rule definition.

- **case-sensitive**
  - Default: Disabled.
  - This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - `operator` must be one of the following:
    - `!`: does not equal
    - `!contains`: does not contain
    - `!ends-with`: does not end with
    - `!starts-with`: does not start with
    - `=`: equals
    - `contains`: contains
    - `ends-with`: ends with
    - `starts-with`: starts with

- **to**
  - Specifies the string for this rule definition.
  - `to` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the “to” field of e-mail in the IMAP message of analyzed state.

**Example**

```
The following command creates IMAP rule definition for analyzing user traffic using occurrence of \textit{xyz.com} in the “to” field of e-mail in the IMAP message:

\texttt{imap to contains xyz.com}
The following commands define rules for analyzing traffic based on Internet Protocol (IP):
**ip any-match**

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for IP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ip any-match [ operator ] [ condition ]
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the IP analyzed state.

**Example**
The following command creates IP rule definition for analyzing user traffic using an IP any match state of `FALSE`:

```
ip any-match = FALSE
```
ip downlink

This command defines a rule definition to analyze and charge user traffic matching the direction of IP packet to downlink (to subscriber).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip downlink operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- ! =: does not equal
- =: equals

condition
Specifies the condition for this rule definition.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the IP packet direction as downlink.

Example
The following command creates IP rule definition for analyzing user traffic using an IP packet direction to downlink (to subscriber):

ip downlink = TRUE
ip dst-address

This command defines a rule definition to analyze and charge user traffic based on IP destination address.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip dst-address { operator { ip_address|ip_address/mask } | { !range | range } host-pool host_pool }

- **no**
  Removes the specified rule definition.

- **operator { ip_address | ip_address/mask }**
  - **operator**: Specifies how to logically match the IP destination address.
  - Must be one of the following:
    - `!=`: does not equal
    - `<=`: less than or equals
    - `=`: equals
    - `>=`: greater than or equals
  - **ip_address**: Specifies IP address of the destination node for outgoing traffic in IPv4 or IPv6 standard notation. `ip_address` must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation.
  - **ip_address/mask**: Specifies IP address of the destination node for outgoing traffic in IPv4 or IPv6 standard notation with subnet mask bit. `ip_address/mask` must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

- **{ !range | range } host-pool host_pool**
  - **!range | range**: Specifies the range criteria:
    - `!range`: Not in the range of
    - `range`: In the range of
  - **host-pool host_pool**: Specifies the host pool name. `host_pool` must be a string of 1 through 63 characters in length.

Usage

Use this command to specify a rule definition to analyze user traffic based on IP destination address.

Example
The following command creates IP rule definition for analyzing user traffic using an IP destination address of 1.1.1.1:

```
ip dst-address = 1.1.1.1
```
ip error

This command defines a rule definition to analyze user traffic for invalid IP packets and other errors while parsing IP packets.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ip error operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - $!=$: does not equal
  - $=$: equals

- **condition**
  Specifies the condition for this rule definition.
  *condition* must be one of the following:
  - *FALSE*
  - *TRUE*

**Usage**

Use this command to define a rule definition to analyze user traffic for invalid IP packets and any other errors while parsing IP packets.

**Example**

The following command creates an IP rule definition for analyzing user traffic using an IP error status of *TRUE*:

```
ip error = TRUE
```
ip protocol

This command defines a rule definition to analyze and charge user traffic based on the protocol being transported by IP packets.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] ip protocol operator{protocol_assignment|protocol }
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the IP protocol.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than equals—available only in StarOS 8.1 and later
  - `=`: Equals
  - `>=`: greater than equals—available only in StarOS 8.1 and later

- **protocol_assignment**
  Specifies the protocol by assignment number.
  `protocol_assignment` must be an integer from 0 through 255.
  For example, 1 for ICMP, 6 for TCP, and 17 for UDP.

- **protocol**
  Specifies the protocol by name. `protocol` must be one of the following:
  - `ah`
  - `esp`
  - `gre`
  - `icmp`
  - `icmpv6`
  - `tcp`
  - `udp`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the IP protocol.
Example
The following command creates IP rule definition for analyzing user traffic using a protocol assignment of 2:

```
ip protocol = 2
```
**ip server-ip-address**

This command defines a rule definition to analyze and charge user traffic matching the IP address of the destination, i.e. from the subscriber, of the connection.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ip server-ip-address { operator { ip_address | ip_address/mask } | { !range | range } host-pool host_pool }
```

- **no**
  Removes the specified rule definition.

- **operator { ip_address | ip_address/mask }**
  **operator**: Specifies how to logically match the server IP address. `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `=>`: greater than or equals

- **ip_address**: Specifies the server IP address in IPv4 or IPv6 standard notation. For uplink packets (from subscriber) this field matches the destination IP address in the IP header, and for downlink packets (to the subscriber) it matches the source IP address in IP header. `ip_address` must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation.

- **ip_address/mask**: Specifies the server IP address in IPv4 or IPv6 standard notation with subnet mask bit. For uplink packets (from subscriber) this field matches the destination IP address in the IP header, and for downlink packets (to the subscriber) it matches the source IP address in IP header. `ip_address/mask` must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

- **{ !range | range } host-pool host_pool**

  **!range | range**: Specifies the range criteria:
  - `!range`: Not in the range of
  - `range`: In the range of

  **host-pool host_pool**: Specifies the host pool name. `host_pool` must be a string of 1 through 63 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the server IP address.
Example
The following command creates an IP rule definition for analyzing user traffic using an IP server address of 1.10.1.1:

```
  ip server-ip-address = 1.10.1.1
```
ip src-address

This command defines a rule definition to analyze and charge user traffic based on IP source address.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip src-address { operator { ip_address | ip_address/mask } | { !range | range } } host-pool host_pool
```

no

Removes the specified rule definition.

```
operator { ip_address | ip_address/mask }
```

operator: Specifies how to logically match the IP source address.

```
operator must be one of the following:
- !: does not equal
- <=: less than or equals
- =: equals
- >=: greater than or equals
```

```
ip_address: Specifies IP address of the source node for incoming traffic in IPv4 or IPv6 standard notation. ip_address must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation.
```

```
ip_address/mask: Specifies IP address of the source node for incoming traffic in IPv4 or IPv6 standard notation with subnet mask bit. ip_address/mask must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.
```

```
{ !range | range } host-pool host_pool
```

```
!range | range: Specifies the range criteria:
- !range: Not in the range of
- range: In the range of
```

```
host-pool host_pool: Specifies the host pool name. host_pool must be a string of 1 through 63 characters in length.
```

Usage

Use this command to specify a rule definition to analyze user traffic based on IP source address.

Example

The following command creates an IP rule definition for analyzing user traffic using an IP source address of 1.1.1.1:
ip src-address = 1.1.1.1
ip subscriber-ip-address

This command defines a rule definition to analyze and charge user traffic matching the IP address of the subscriber (either source address or destination address).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip subscriber-ip-address { operator { ip_address | ip_address/mask } | { !range | range } host-pool host_pool }

no
Removes the specified rule definition.

operator { ip_address | ip_address/mask }
operator: Specifies how to logically match the subscriber IP address.
operator must be one of the following:
  • ! =: does not equal
  • <=: less than or equals
  • =: equals
  • >=: greater than or equals

ip_address: Specifies the subscriber IP address. Depending on the direction of packet this IP address will be either the IP source address or the IP destination address. ip_address must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation.
ip_address/mask: Specifies the subscriber IP address with subnet mask bit. Depending on the direction of packet this IP address will either be the IP source address or the IP destination address.
ip_address/mask must be an IPv4 address in dotted decimal notation, or an IPv6 address in colon notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool host_pool

!range | range: Specifies the range criteria:
  • !range: Not in the range of
  • range: In the range of

host-pool host_pool: Specifies the host pool name. host_pool must be a string of 1 through 63 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on the subscriber IP address.
Example
The following command creates an IP rule definition for analyzing user traffic using an IP address of 161.10.1.1 for subscriber:

```
ip subscriber-ip-address = 161.10.1.1
```
ip total-length

This command defines a rule definition to analyze and charge user traffic based on IP total length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip total-length operator total_length

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `>=`: greater than or equals

- **total_length**
  Specifies the total length of the IP packet including payload that is for this rule definition. 
  `total_length` must be an integer from 0 through 4096.

Usage

Use this command to specify a rule definition to analyze user traffic based on the IP total length.

Example

The following command creates an IP rule definition for analyzing user traffic using an IP total length of 2000 bytes:

```
ip total-length = 2000
```
ip uplink

This command defines a rule definition to analyze and charge user traffic matching the direction of IP packet to uplink (from subscriber).

Product

All

Privilege

Security Administrator, Administrator

Syntax

[ no ] ip uplink operator condition

no

Removes the specified rule definition.

operator

Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- ! =: does not equal
- =: equals

condition

Specifies the condition for this rule definition. condition must be one of the following:

- FALSE
- TRUE

Usage

Use this command to specify a rule definition to analyze user traffic based on the IP packet direction as uplink.

Example

The following command creates IP rule definition for analyzing user traffic using an IP packet direction to uplink (from subscriber):

    ip uplink = TRUE
ip version

This command defines a rule definition to analyze and charge user traffic based on the IP version.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip version operator ip_version

**no**
Removes the specified rule definition.

**operator**
Specifies how to logically match information in the analyzed field. 
operator must be = (equals).

**ip_version**
Specifies the IP version. ip_version must be one of the following:
-IPv4
-IPv6

Usage
Use this command to define a rule definition to analyze and charge user traffic based on the IP version.

Example
The following command creates an IP rule definition to analyze user traffic for the IP version IPv6:

```
ip version = ipv6
```
mms

The following commands define rules for analyzing traffic based on Multimedia Messaging Service (MMS):
mms any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for MMS.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms any-match operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• ! =: does not equal
• =: equals

condition
Specifies the condition for this rule definition.
condition must be one of the following:
• FALSE
• TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the mms any match status.

Example
The following command creates an MMS rule definition for analyzing user traffic using an MMS any match status of FALSE:

mms any-match = FALSE
mms bcc

This command defines a rule definition to analyze and charge user traffic based on MMS Blind Carbon Copy (BCC).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms bcc [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• !contains: does not contain
• !ends-with: does not end with
• !starts-with: does not start with
• ==: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

string
Specifies the string for this rule definition.
string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on an MMS BCC value.

Example
The following command creates an MMS rule definition for analyzing user traffic containing an MMS BCC value of test1:

mms bcc test1
mms bcc contains test1
mms cc

This command defines a rule definition to analyze and charge user traffic based on the Carbon Copy (cc) field of MMS message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] mms cc [ case-sensitive ]operator string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  The operator must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  Specifies the string for this rule definition.
  The string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on an MMS cc value.

Example
The following command creates an MMS rule definition for analyzing user traffic containing an MMS CC value of test1:

```
mms cc contains test1
```
mms content location

This command defines a rule definition to analyze and charge user traffic based on MMS content location.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
[ no ] mms content location [ case-sensitive ] operator string
```

**no**
Removes the specified rule definition.

**case-sensitive**
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

**operator**
Specifies how to logically match the information in the analyzed field.

- `!=`: does not equal
- `!contains`: does not contain
- `!ends-with`: does not end with
- `!starts-with`: does not start with
- `=`: equals
- `contains`: contains
- `ends-with`: ends with
- `starts-with`: starts with

**string**
Specifies the string for this rule definition.

*string* must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on an MMS content location value.

Example
The following command creates an MMS rule definition for analyzing user traffic containing an MMS content location value of test1:

```
mms content location contains test1
```
mms content type

This command defines a rule definition to analyze and charge user traffic based on MMS content type.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] mms content type [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  Specifies the string for this rule definition.
  *string* must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on an MMS “content-type” field value.

Example

The following command creates an MMS rule definition for analyzing user traffic containing an MMS content type as `image`: 
mms content type contains image
mms downlink

This command defines the rule definition to analyze and charge user traffic based on MMS message downlink condition.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms downlink operator condition

no
Removes the specified rule definition.

operator
 Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- ==: equals

condition
Indicates the downlink (from the Mobile Node direction) status. condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on an MMS downlink status.

Example
The following command creates an MMS rule definition for analyzing user traffic with an MMS downlink value to TRUE:

mms downlink = TRUE
**mms from**

This command defines the rule definition to analyze and charge user traffic based on the from field in MMS message.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] mms from [ case-sensitive ] operator string
```

- **no**
  
  Removes the specified rule definition.

- **case-sensitive**
  
  Default: Disabled.
  
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  
  Specifies how to logically match the information in the analyzed field.
  
  `operator` must be one of the following:
  
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with` : ends with
  - `starts-with`: starts with

- **string**
  
  Specifies the string for this rule definition.
  
  `string` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the “from” field of an MMS message.

**Example**

...
The following command creates an MMS rule definition for analyzing user traffic containing `test1` in the “from” field of MMS message:

```
mms from contains test1
```
mms message-id

This command defines a rule definition to analyze and charge user traffic based on the “message-id” of an MMS message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms message-id [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

• !=: does not equal
• !(contains): does not contain
• !(ends-with): does not end with
• !(starts-with): does not start with
• ==: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

string
Specifies the string for this rule definition.
string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on an MMS message ID value.

Example
The following command creates an MMS rule definition for analyzing user traffic containing an MMS message ID of test1:

```
mms message-id contains test1
```
mms pdu-type

This command defines a rule definition to analyze and charge user traffic based on the MMS Protocol Data Unit (PDU) type.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms pdu-type operator pdu_type

- no
  Removes the specified rule definition.

- operator
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  • !=: does not equal
  • ==: equals

- pdu_type
  Specifies the MMS PDU type used for this rule definition.
  pdu_type must be one of the following:
  • mms-pdu-type-m-acknowledge-ind
  • mms-pdu-type-m-delivery-ind
  • mms-pdu-type-m-http-get
  • mms-pdu-type-m-notification-ind
  • mms-pdu-type-m-notify-rsp-ind
  • mms-pdu-type-m-retrieve-conf
  • mms-pdu-type-m-send-conf
  • mms-pdu-type-m-send-request
  • mms-pdu-type-m-wsp-get
  • mms-pdu-type-m-response

Usage
Use this command to specify a rule definition to analyze user traffic based on type of an MMS PDU.

Example
The following command creates an MMS rule definition for analyzing user traffic for MMS PDU:

```
  mms_pdu-type = mms_pdu-type-m-http-get
```
**mms previous-state**

This command defines a rule definition to analyze and charge user traffic based on MMS previous state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] mms previous-state operator previous_state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **previous_state**
  Analyzes the previous state of the MMS transmissions.
  `previous_state` must be one of the following:
  - `delayed-ack-pending`
  - `delayed-m-notify-rsp-sent`
  - `delayed-retrieval-pending`
  - `immediate-retrieval-pending`
  - `init`
  - `m-send-conf-rcvd`
  - `m-send-req-sent`
  - `notification-ind-rcvd`
  - `notify-rsp-sent`
  - `retrieval-pending`
  - `retrieved-conf-received`
  - `send-success`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an MMS previous state.
Example

The following command creates an MMS rule definition for analyzing user traffic using an MMS previous state of retrieval-pending:

```
mms previous-state = retrieval-pending
```
mms response status

This command defines a rule definition to analyze and charge user traffic based on MMS response status code.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms response status operator status_code

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !: does not equal
- := equals

status_code
Specifies the code for this rule definition. status_code must be an integer from 128 through 136.

Usage
Use this command to specify a rule definition to analyze user traffic based on an MMS response status.

Example
The following command creates an FTP rule definition for analyzing user traffic using an MMS response status code of 129:

mms response status != 129
mms state

This command defines a rule definition to analyze and charge user traffic based on the current state of MMS message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[m no] mms state operator mms state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- <: equals

mms state
Analyzes the state of the mms transmissions. mms_state must be one of the following:
- delayed-ack-pending
- delayed-m-notify-rsp-sent
- delayed-retrieval-pending
- delivery-failed
- delivery-success
- immediate-retrieval-pending
- m-send-conf-rcvd
- m-send-req-sent
- notification-ind-rcvd
- notify-rsp-sent
- retrieval-failed
- retrieval-pending
- retrieval-success
- retrieve-conf-received
- send-success
Usage
Use this command to specify a rule definition to analyze user traffic based on current state of MMS message.

Example
The following command creates an MMS rule definition for analyzing user traffic using current state of MMS message as `retrieval-failed`:

```
mms state = retrieval-failed
```
mms status

This command defines a rule definition to analyze and charge user traffic based on MMS status.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[ \text{[ no ] mms status} \\text{operator status} \]

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  - \( \text{!}= \): does not equal
  - \( = \): equals

- **status**
  Specifies the status for this rule definition.
  \( \text{status} \) must be an integer from 128 through 132.

Usage

Use this command to specify a rule definition to analyze user traffic based on an MMS status.

Example

The following command creates an MMS rule definition for analyzing user traffic using an MMS status of 130:

\[ \text{mms status} = 130 \]
mms subject

This command defines a rule definition to analyze and charge user traffic using “subject” field of MMS message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms subject [ case-sensitive ]operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field. 
operator must be one of the following:
  • !=: does not equal
  • !contains: does not contain
  • !ends-with: does not end with
  • !starts-with: does not start with
  • ==: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

string
Specifies the string for this rule definition. 
string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on “subject” field of an MMS message.

Example
The following command creates an MMS rule definition for analyzing user traffic for occurrence of test1 in “subject” field of MMS message:

```
mms subject contains test1
```
mms tid

This command defines a rule definition to analyze and charge user traffic based on MMS Transaction Identifier (tid).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] mms tid [ case-sensitive ] operator tid_value
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **tid_value**
  The value of the specified field.
  `tid_value` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on an MMS TID.

**Example**
The following command creates a rule definition for analyzing user traffic using an MMS TID value of test:
mms tid = test
**mms to**

This command defines a rule definition to analyze and charge user traffic using “to” field of MMS message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] mms to[ case-sensitive ]operator to_value
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **to_value**
  The value of the specified field.
  `to_value` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an MMS to rule definition.

**Example**

The following command creates a rule definition for analyzing user traffic using an MMS to value of `test`: 
mms to = test
mms uplink

This command defines a rule definition to analyze and charge user traffic based on MMS uplink.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[
\text{[ no ] mms uplink operator condition}
\]

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - \(\neg\) equals
  - \(=\) equals

- **condition**
  Indicates the uplink (from the Mobile Node direction) status.
  - **FALSE**
  - **TRUE**

Usage
Use this command to specify a rule definition to analyze user traffic based on the MMS uplink.

Example
The following command creates a rule definition for analyzing user traffic using an MMS uplink value of \text{TRUE}:

\[
\text{mms uplink} = \text{TRUE}
\]
mms version

This command defines a rule definition to analyze and charge user traffic based on MMS version.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] mms version operator version

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

  • !=: does not equal
  • ==: equals

version
Specifies the version for this rule definition.
version must be an integer from 1 through 65535.

Important: MMS Protocol Analyzer supports decoding of MMS version 1.0 only.

Usage
Use this command to specify a rule definition to analyze user traffic based on the MMS version.

Example
The following command creates a rule definition for analyzing user traffic using an MMS version of 1.0:

    mms version = 1.0
multi-line-or all-lines

Defines whether to apply the OR operator to all lines in a rule definition.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] multi-line-or all-lines
```

- **no**
  Removes the previous configuration.

Usage
If multi-line-or is enabled for a rule definition, the logical OR operator to all the rule-lines in the rule definition is applied to decide if the rule definition matches or not. If multi-line-or is not configured, the logical AND operator is applied.
p2p

The following commands define rules for analyzing traffic based on Peer-to-Peer protocols:
p2p any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for Peer to Peer (P2P).

Product
ECS

Privilege
Administrator, Config-administrator

Syntax

[ no ] p2p any-match operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • =: equals

condition
Specifies the condition for this rule definition.
condition must be one of the following:
  • TRUE: The rule matches any P2P traffic.
  • FALSE: The rule does not match any P2P traffic.

Usage
Use this command to specify a rule definition to analyze user traffic based on the P2P any match status.

Example
The following command creates a rule definition for analyzing user traffic using an P2P any match status of TRUE:

p2p any-match = TRUE
**p2p protocol**

This command configures the system to detect specific P2P protocols for charging purposes. This command is not used for detection purposes.

**Product**
ECS

**Privilege**
Administrator, Config-administrator

**Syntax**

```plaintext
[ no ] p2p protocol operator protocol
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be `=` (equals).

- **protocol**
  Specifies the protocol for charging purposes. `protocol` must be one of the following:
  - actsync
  - aimini
  - applejuice
  - ares
  - battlefld
  - bittorrent
  - dblink
  - directconnect
  - edonkey
  - fasttrack
  - feidian
  - filetopia
  - freenet
  - fring
  - gadugadu
  - gnutella
  - gtalk
  - halflife2
• hamachivpn
• iax
• imesh
• iptv
• irc
• iskoot
• jabber
• manolito
• msn
• mute
• nimbu
• oovoo
• openft
• orb
• oscar
• paltalk
• pando
• pandora
• popo
• pplive
• ppstream
• qq
• qqgame
• qqlive
• quake
• rdp
• secondlife
• skinny
• skype
• slingbox
• sopcast
• soulseek
• steam
• tvants
• tvuplayer
• uusee
• vpnx
vtun
warcft3
winmx
winnny
wofwarcraft
xbox
yahoo
zattoo

Usage
Use this command to configure detection of protocols for charging purposes. For detection purposes use the `p2p detection protocol` in the Active Charging Service Configuration Mode.

Example
The following command configures the system to detect orb protocol for charging purposes:

```
p2p protocol = orb
```
p2p traffic-type

This command defines a rule definition to analyze and charge user traffic based on the type of traffic, such as voice or non-voice.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] p2p traffic-type operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

• ! =: does not equal
• =: equals

condition
Specifies the condition for this rule definition. condition must be one of the following:

• voice

Usage
Use this command to configure the system to detect voice or non-voice P2P traffic. When the detection of a protocol is enabled then the detection of sub-type is enabled by default.

Example
The following command configures the system to detect voice traffic:

p2p traffic-type = voice
pop3

The following commands define rules for analyzing traffic based on Post Office Protocol 3 (POP3):
pop3 any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for POP3.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] pop3 any-match [ operator condition ]
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the POP3 any match status.

**Example**
The following command creates an POP3 rule definition for analyzing user traffic using a POP3 any match status of `FALSE`:

```
pop3 any-match = FALSE
```
pop3 command args

This command defines a rule definition to analyze and charge user traffic based on the POP3 command arguments.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] pop3 command args [ case-sensitive ] operator argument

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • !=: does not equal
  • !contains: does not contain
  • !ends-with: does not end with
  • !starts-with: does not start with
  • ==: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

argument
A unique value that you specify to use for the command argument.
argument must be an alpha and/or numeric string of 1 through 40 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on a POP3 command argument.

Example
The following command defines a rule definition for analyzing POP3 user traffic using a command argument of test:
pop3 command args = test
pop3 command id

This command defines a rule definition to analyze and charge user traffic based on the POP3 command ID.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] pop3 command id operator command_id

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• <=: less than or equals
• ==: equals
• >=: greater than or equals

command_id
A unique value that you specify to use for the command argument.
command_id must be an integer from 1 through 12.

Usage
Use this command to specify a rule definition to analyze user traffic based on a POP3 command ID.

Example
The following command defines a rule definition for analyzing POP3 user traffic using a command ID of 8:

pop3 command id = 8
pop3 command name

This command defines a rule definition to analyze and charge user traffic based on the POP3 command name.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] pop3 command name operator command_name

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- ! =: does not equal
- =: equals

command_name
command_name must be one of the following:
- apop
- dele
- list
- noop
- pass
- quit
- retr
- reset
- stat
- top
- uid1
- user

Usage
Use this command to specify a rule definition to analyze user traffic based on a POP3 command name.
The following command defines a rule definition for analyzing POP3 user traffic using a command name of \textit{list}:

\begin{verbatim}
pop3 command name = list
\end{verbatim}
pop3 mail-size

This command defines a rule definition to analyze and charge user traffic based on the POP3 mail size.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
{ no } pop3 mail-size {operator mail_size | { { range | !range }
rangle_from to range_to} }
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- `{ range | !range } range_from to range_to`
  Enables or disables the range criteria.
  `range`: Enables the range criteria.
  `!range`: Disables the range criteria.
  `range_from` specifies the start of range, and must be an integer from 1 through 4000000000.
  `range_to` specifies the end range. `range_to` must be an integer from 1 through 4000000000, and must be greater than `range_from`.

- **mail_size**
  Specifies the mail size for this rule definition.
  `mail_size` must be an integer from 1 through 4000000000.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on POP3 mail size.

**Example**

The following command defines a rule definition for analyzing POP3 user traffic using a mail size of 40000:

```plaintext
pop3 mail-size = 40000
```
pop3 mail-size

Ruledef Configuration Mode Commands
**pop3 pdu-length**

This command defines a rule definition to analyze and charge user traffic based on the POP3 Protocol Data Unit (PDU) length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] pop3 pdu-length { operator pdu_length | { range | !range
range_from to range_to } }
```

**no**
Removes the specified rule definition.

**operator**
Specifies how to logically match the information in the analyzed field.

- `!=`: does not equal
- `<=`: less than or equals
- `=`: equals
- `>=`: greater than or equals

```
{ range | !range } range_from to range_to
```

Enables or disables the range criteria.

- **range**: Enables the range criteria.
- **!range**: Disables the range criteria.

- **range_from**: Specifies the start of range, and must be an integer from 0 through 65535.
- **range_to**: Specifies the end range. **range_to** must be an integer from 0 through 65535, and must be greater than **range_from**

**pdu_length**
Specifies the POP3 PDU length for this rule definition.

**pdu_length** must be an integer from 0 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a POP3 PDU length (header + payload) in bytes.

**Example**
The following command defines a rule definition for analyzing POP3 user traffic using a PDU length of 1000 bytes:

```
pop3 pdu-length = 1000
**pop3 pdu-type**

This command defines a rule definition to analyze and charge user traffic based on the POP3 PDU type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] pop3 pdu-type operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  Specifies the packet type for this rule definition.
  `condition` must be one of the following:
  - `command-packet`
  - `data-packet`
  - `relay-packet`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a POP3 PDU type.

**Example**
The following command defines a rule definition for analyzing POP3 user traffic using a PDU type of `relay-packet`:

```
pop3 pdu-type = relay-packet
```
**pop3 previous-state**

This command defines a rule definition to analyze and charge user traffic based on the POP3 previous state.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] pop3 previous-state operator previous-state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - `!`: does not equal
  - `=`: equals

- **previous_state**
  Specifies the previous state for this rule definition.
  **previous_state** must be one of the following:
  - `connected`: connected state
  - `data transaction`: data transaction state
  - `init`: initialized state
  - `reply-error`: reply error state
  - `reply-ok`: response ok state
  - `waiting-for-reply`: waiting for reply state

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a POP3 previous state.

**Example**

The following command creates a POP3 rule definition for analyzing user traffic using a POP3 previous state of `connected`:

```
pop3 previous-state = connected
```
pop3 reply args

This command defines a rule definition to analyze and charge user traffic based on the POP3 reply arguments.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[ \text{no } \] \text{pop3 reply args [ case-sensitive ]operator argument} \]

- \text{no}
  Removes the specified rule definition.

- \text{case-sensitive}
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- \text{operator}
  Specifies how to logically match the information in the analyzed field.
  \text{operator} must be one of the following:
  - \text{!=}: does not equal
  - \text{!contains}: does not contain
  - \text{!ends-with}: does not end with
  - \text{!starts-with}: does not start with
  - \text{=} : equals
  - \text{contains}: contains
  - \text{ends-with}: ends with
  - \text{starts-with}: starts with

- \text{argument}
  A unique value that you specify to use for the reply argument.
  \text{argument} must be an alpha and/or numeric string of 1 through 512 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on a POP3 reply argument rule definition.

Example
The following command defines a rule definition for analyzing POP3 user traffic using a reply argument of \text{test}:
pop3 reply args = test
pop3 reply id

This command defines a rule definition to analyze and charge user traffic based on the POP3 reply ID.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] pop3 reply id operator reply_id

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- :=: equals

reply_id
Specifies the reply ID for this rule definition. reply_id must be one of the following:
- 0: Unknown reply
- 1: +OK reply
- 2: -ERR reply

Usage
Use this command to specify a rule definition to analyze user traffic based on a POP3 reply ID.

Example
The following command defines a rule definition for analyzing POP3 user traffic using a reply ID of 2:

```bash
pop3 reply id = 2
```
pop3 reply status

This command defines a rule definition to analyze and charge user traffic based on the POP3 reply status.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[ no ] pop3 reply status operator reply_status

---

no

Removes the specified rule definition.

---

operator

Specifies how to logically match the information in the analyzed field. 
operator must be one of the following:

- !=: does not equal
- ==: equals

---

reply_status

Specifies the reply ID for this rule definition.
reply_status must be one of the following:

- +OK: reply OK
- -ERR: reply error

Usage

Use this command to specify a rule definition to analyze user traffic based on a POP3 reply status.

Example

The following command defines a rule definition for analyzing POP3 user traffic using a reply status of +OK:

pop3 reply status = +ok
pop3 session-length

This command defines a rule definition to analyze and charge user traffic based on the POP3 session length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
{ no | pop3 session-length { operator session_length | { range | !range } range_from to range_to }

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !=: does not equal
- <=: less than or equals
- =: equals
- >=: greater than or equals

session_length
Specifies the session length used for this rule definition.
session_length must be an integer from 1 through 400000000.

{ range | !range } range_from to range_to
Enables or disables the range criteria for PoP3 session length.
range: Enables the range criteria for Pop3 session length.
!range: Disables the range criteria for PoP3 session length.
range_from: Specifies the start of range of PoP3 session length, and must be an integer from 1 through 400000000 but less than or equal to range_to.
range_to: Specifies the end of range of PoP3 session length, and must be an integer from 1 through 400000000 but greater than or equal to range_from
```

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the POP3 session length.

**Example**
The following command creates a POP3 rule definition for analyzing user traffic using a POP3 session length of 40000:
pop3 session-length = 40000
**pop3 state**

This command defines a rule definition to analyze and charge user traffic based on the POP3 state.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
[ no ] pop3 state operator state
```

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - `!=`: does not equal
  - `==`: equals

- **state**
  - Specifies the POP3 state for this rule definition.
  - `state` must be one of the following:
    - `close`
    - `connected`
    - `data-transaction`
    - `reply-error`
    - `reply-ok`
    - `waiting-for-reply`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a POP3 state.

**Example**

The following command creates a POP3 rule definition for analyzing user traffic using a POP3 state of `close`:

```
pop3 state = close
```
### pop3 user-name

This command defines a rule definition to analyze and charge user traffic based on the POP3 user name.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] pop3 user-name [ case-sensitive ] operator user_name
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **user_name**
  A unique value that you specify to use for the user name.
  `user_name` must be an alpha and/or numeric string of 1 through 64 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a POP3 username rule definition.

**Example**

The following command defines a rule definition for analyzing POP3 user traffic using a user name of `test`:
pop3 user-name = test
The following commands define rules for analyzing traffic based on the Real-time Transport Control Protocol (RTCP):
**rtcp any-match**

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for RTCP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtcp any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `TRUE`: The rule matches any RTCP traffic
  - `FALSE`: The rule does not match any RTCP traffic

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the RTCP any match status.

**Example**
The following command creates a rule definition for analyzing user traffic using an RTCP any match status of `TRUE`:

```
rtcp any-match = TRUE
```
rtcp jitter

This command defines a rule definition to analyze and charge user traffic based upon the amount of jitter in the RTCP protocol.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtcp jitter operator value

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - !: does not equal
  - <: less than or equals
  - =: equals
  - =>: greater than or equals

- **value**
  This value represents the amount of jitter to test against.
  *value* must be an integer from 0 through 4294967295.

Usage

Use this command to set a rule based on the jitter in the RTCP protocol.

Example

The following command test for jitter greater than or equal to 12954:

```
rtcp jitter >= 12954
```
rtcp parent-proto

This command defines a rule definition to analyze and charge user traffic based on the parent protocol of the RTCP flow.

**Important:** This command is only available in StarOS 8.1 and StarOS 9.0 and later.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtcp parent-proto operator parent_protocol
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **parent_protocol**
  Specifies the RTCP parent protocol for this rule definition.
  `parent_protocol` must be one of the following:
  - `rtsp`: Real Time Streaming Protocol
  - `sip`: Session Initiation Protocol

**Usage**

Use this command to specify a rule definition to analyze and charge user traffic based on the parent protocol of the RTCP flow.

**Example**

The following command creates an RTCP rule definition to analyze user traffic based on the parent protocol of the RTCP flow being SIP:

```
rtcp parent-proto = sip
```
**rtcp pdu-length**

This command defines a rule definition to analyze and charge user traffic based upon the Real-time Transport Protocol (RTCP) Protocol Data Unit (PDU) length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
[ no ] rtcp pdu-length operator pdu_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `>=`: greater than or equals

- **pdu_length**
  Specifies the RTCP length, in bytes, for this rule definition.
  In StarOS 8.1 and later, `pdu_length` must be an integer from 1 through 65535. In StarOS 8.0, `pdu_length` must be an integer from 1 through 2000.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on an RTCP PDU length (header + payload) in bytes.

**Example**
The following command creates a rule definition for analyzing user traffic using an RTCP PDU length of 10000 bytes:
```
rtcp pdu-length = 10000
```
**rtcp rtsp-id**

This command defines a rule definition to analyze and charge user traffic using a RTSP ID associated with Real-time Transport Control Protocol (RTCP).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtcp rtsp-id [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - `!`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  Specifies the string for this rule definition.
  **string** must be an alpha and/or numeric string of 1 through 32 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an MMS message ID value.

**Example**

The following command creates an RTCP rule definition for analyzing user traffic containing an RTSP message ID of `test1`:
rtcp rtsp-id contains test1
rtcp session-length

This command defines a rule definition to analyze and charge user traffic based on the Real-time Transport Protocol (RTCP) session length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtcp session-length operator session_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `>=`: greater than or equals

- **session_length**
  Specifies the RTCP total session length for this rule definition.
  In StarOS 8.1 and later, `session_length` must be an integer from 1 through 4000000000. In StarOS 8.0, `session_length` must be an integer from 1 through 40000000.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the RTCP total session length.

**Example**

The following command creates an RTCP rule definition for analyzing user traffic using a total RTCP session length of 200000:

```
rtcp session-length = 200000
```
rtcp uri

This command defines a rule definition to analyze and charge user traffic using uniform resource identifier (URI) associated with Real-time Transport Control Protocol (RTCP).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtcp uri [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !: does not equal
- !contains: does not contain
- !ends-with: does not end with
- !starts-with: does not start with
- =: equals
- contains: contains
- ends-with: ends with
- starts-with: starts with

string
Specifies the string for this rule definition.
string must be an alpha and/or numeric string of 1 through 127 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on an RTCP URI.

Example
The following command creates an RTP rule definition for analyzing user traffic using an RTCP URI string of rtsp://www.example.org:
rtcp uri = rtsp://www.example.org
rtp

The following commands define rules for analyzing traffic based on the Real-time Transport Protocol (RTP):
rtp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for RTP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtp any-match operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
  • !=: does not equal
  • ==: equals

condition
Specifies the condition for this rule definition. condition must be one of the following:
  • FALSE
  • TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the RTP any match status.

Example
The following command creates an MMS rule definition for analyzing user traffic using an RTP any match status of TRUE:

rtp any-match = TRUE
rtp parent-proto

This command defines a rule definition to analyze and charge user traffic based on the parent protocol of the RTP flow.

**Important:** This command is only available in StarOS 8.1 and StarOS 9.0 and later.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtp parent-proto operator parent_protocol
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **parent_protocol**
  Specifies the RTP parent protocol for this rule definition. 
  `parent_protocol` must be one of the following:
  - `rtsp`: Real Time Streaming Protocol
  - `sip`: Session Initiation Protocol

**Usage**

Use this command to specify a rule definition to analyze and charge user traffic based on the parent protocol of the RTP flow.

**Example**

The following command creates an RTP rule definition to analyze user traffic based on the parent protocol of the RTP flow being SIP:

```
rtp parent-proto = sip
```
**rtp pdu-length**

This command defines a rule definition to analyze and charge user traffic based on the RTP Protocol Data Unit (PDU) length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] rtp pdu-length [operator pdu_length]
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=": equals
  - `>=": greater than or equals

- **pdu_length**
  Specifies the RTP PDU length, in bytes, for this rule definition.
  In StarOS 8.1 and later, `pdu_length` must be an integer from 1 through 65535. In StarOS 8.0, `pdu_length` must be an integer from 1 through 2000.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on an RTP PDU length (header + payload) in bytes.

**Example**
The following command creates an HTTP rule definition for analyzing user traffic using an RTP PDU length of 1000 bytes:

```plaintext
rtp pdu-length = 1000
```
rtp rtsp-id

This command defines a rule definition to analyze and charge user traffic based on the RTSP ID associated with RTP flow.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtp rtsp-id [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• !contains: does not contain
• !ends-with: does not end with
• !starts-with: does not start with
• =: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

string
Specifies the string for this rule definition.
string must be an alpha and/or numeric string of 1 through 32 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on an MMS message ID value.

Example
The following command creates an RTP rule definition for analyzing user traffic containing an RTSP message ID of test1:
rtp rtsp-id contains test1
**rtp session-length**

This command defines a rule definition to analyze and charge user traffic based on RTP session length.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] rtp session-length operator session_length
```

- **no**
  
  Removes the specified rule definition.

- **operator**
  
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **session_length**
  
  Specifies the RTP total session length for this rule definition. In StarOS 8.1 and later, `session_length` must be an integer from 1 through 4000000000. In StarOS 8.0, `session_length` must be an integer from 1 through 4000000.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the RTP total session length.

**Example**

The following command creates an RTP rule definition for analyzing user traffic using a total RTP session length of 200000:

```
rtp session-length = 200000
```
rtp uri

This command defines a rule definition to analyze and charge user traffic based on the uniform resource identifier (URI) associated with RTP flow.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtp uri [ case-sensitive ] operator string

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>case-sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: Disabled. This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field. operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: does not equal</td>
</tr>
<tr>
<td>• !contains: does not contain</td>
</tr>
<tr>
<td>• !ends-with: does not end with</td>
</tr>
<tr>
<td>• !starts-with: does not start with</td>
</tr>
<tr>
<td>• ==: equals</td>
</tr>
<tr>
<td>• contains: contains</td>
</tr>
<tr>
<td>• ends-with: ends with</td>
</tr>
<tr>
<td>• starts-with: starts with</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>string</th>
</tr>
</thead>
<tbody>
<tr>
<td>A unique name that you specify for the RTP URI. string must be an alpha and/or numeric string of 1 through 127 characters in length. string allows punctuation characters and it does not include the “host” portion.</td>
</tr>
</tbody>
</table>

Usage

Use this command to specify a rule definition to analyze user traffic based on an RTP URI.

Example
The following command creates an RTP rule definition for analyzing user traffic using an RTP URI string of \textit{rtsp://www.example.org}:

\texttt{rtp uri} = \texttt{rtsp://www.example.org}
rtsp

The following commands define rule for analyzing traffic based on Real Time Streaming Protocol (RTSP):
rtsp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for RTSP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp any-match operator condition

---

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- ==: equals

condition
Specifies the condition for this rule definition. condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the RTSP any match status.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP any match status of FALSE.

rtsp any-match = FALSE
rtsp content length

This command defines a rule definition to analyze and charge user traffic based on RTSP content length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtsp content length operator content_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `>=`: greater than or equals

- **content_length**
  Specifies the RTSP body length, in bytes, for this rule definition. `content_length` must be an integer from 0 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an RTSP content length.

**Example**

The following command creates an RTSP rule definition for analyzing user traffic using an RTSP body length of 10000:

```
rtsp content length = 10000
```
rtsp content type

This command defines a rule definition to analyze and charge user traffic based on RTSP content type.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp content type [ case-sensitive ]operator content_type

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • !=: does not equal
  • !contains: does not contain
  • !ends-with: does not end with
  • !starts-with: does not start with
  • =: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

content_type
A unique name that you specify for the RTSP content type.
content_type must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on an RTSP content type.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP content type of abc100:
rtsp content type = abc100
rtsp date

This command defines a rule definition to analyze and charge user traffic matching the ‘date’ field in the RTSP message type.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp date [ case-sensitive ] operator date_string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

• !=: does not equal

• !=contains: does not contain

• !=ends-with: does not end with

• !=starts-with: does not start with

• =: equals

• contains: contains

• ends-with: ends with

• starts-with: starts with

date_string
A unique name that you specify for the date in RTSP header.
content_type must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic matching date string in RTSP header.

Example
The following command creates an RTSP rule definition for analyzing user traffic using a match for date string of 12_04_2006 in RTSP message header:

\texttt{rtsp date = 12\_04\_2006}
rtsp previous-state

This command defines a rule definition to analyze and charge user traffic based on RTSP previous state.

Product
- All

Privilege
- Security Administrator, Administrator

Syntax

```plaintext
[ no ] rtsp previous-state operator previous_state
```

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - `!`: does not equal
  - `=`: equals

- **previous_state**
  - Specifies the RTSP previous state for this rule definition.
  - `previous_state` must be one of the following:
    - `init`
    - `open`
    - `play`
    - `ready`
    - `record`

Usage

Use this command to specify a rule definition to analyze user traffic based on an RTSP previous state.

Example

The following command creates an RTSP rule definition for analyzing user traffic using an RTSP previous state of `ready`:

```plaintext
rtsp previous-state = ready
```
rtsp reply code

This command defines a rule definition to analyze and charge user traffic based on RTSP reply.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[ \text{[ no ] rtsp reply code} \ \text{operator code} \]

\text{no}
Removes the specified rule definition.

\text{operator}
Specifies how to logically match the information in the analyzed field. \text{operator} must be one of the following:
- \text{!#}: does not equal
- \text{<=}: less than or equals
- \text{==}: equals
- \text{>=}: greater than or equals

\text{code}
Specifies the RTSP response for this rule definition. \text{code} must be an integer from 100 through 599.

Usage
Use this command to specify a rule definition to analyze user traffic based on an RTSP return code.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP return code of 356:

\text{rtsp reply code} = 356
rtsp request method

This command defines a rule definition to analyze and charge user traffic based on RTSP method.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] rtsp request method operator method
```

**no**
Removes the specified rule definition.

**operator**
Specifies how to logically match the information in the analyzed field.
**operator** must be one of the following:
- `!`: does not equal
- `=`: equals

**method**
Specifies the RTSP method for this rule definition.
**method** must be one of the following requests:
- `announce`
- `describe`
- `get-parameter`
- `options`
- `pause`
- `play`
- `record`
- `redirect`
- `set-parameter`
- `setup`
- `teardown`

Usage
Use this command to specify a rule definition to analyze user traffic based on an RTSP method.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP method of announce:

\[ \text{rtsp request method} = \text{announce} \]
rtsp request packet

This command defines a rule definition to analyze and charge user traffic based on RTSP request packet.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp request packet operator condition

---

no

Removes the specified rule definition.

---

operator

Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- !=: does not equal
- ==: equals

---

condition

Specifies the condition for this rule definition. condition must be one of the following:

- TRUE: is request
- FALSE: is response

---

Usage

Use this command to specify a rule definition to analyze user traffic based on an RTSP request packet.

---

Example

The following command creates an RTSP rule definition for analyzing user traffic using an RTSP response packet:

    rtsp request packet != FALSE
**rtsp rtp-seq**

This command defines a rule definition to analyze and charge user traffic based on sequence “seq” field in the RTP-Info header of the RTSP message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtsp rtp-seq operator time_stamp
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **string**
  A unique name that you specify to match with the ‘seq’ field in RTP-Info header of the RTSP message.
  `string` must be an alpha and/or numeric string of 0 through 65535 characters in Normal Play Time (NPT) time format.

**Usage**

Use this command to specify a rule definition to analyze user traffic matching the sequence ‘seq’ field in the RTP-Info header of the RTSP response for a PLAY request.

**Example**

The following command creates an RTSP rule definition for analyzing user traffic using an RTP-seq of 2348:

```
rtsp rtp-seq = 2348
```
rtsp rtp-time

This command defines a rule definition to analyze and charge user traffic based on ‘time’ field in the RTP-Info header of the RTSP message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp rtp-time operator time_stamp

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !: does not equal
- <=: less than or equals
- =: equals
- >>: greater than or equals

string
A unique name that you specify to match with the ‘time’ field in RTP-Info header of the RTSP message. string must be an alpha and/or numeric string of 1 through 2147483647 characters in Normal Play Time (NPT) time format.

Usage
Use this command to specify a rule definition to analyze user traffic matching the ‘time’ field in the RTP-Info header of the RTSP response for a PLAY request.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTP-Time-stamp of 19970123T153600Z:

rtsp rtp-time = 19970123T153600Z
rtsp rtp-uri

This command defines a rule definition to analyze and charge user traffic based on the uniform resource identifier (URI) field in the RTP-Info header of the RTSP message.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp rtp-uri [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !=: does not equal
- !contains: does not contain
- !ends-with: does not end with
- !starts-with: does not start with
- =: equals
- contains: contains
- ends-with: ends with
- starts-with: starts with

string
A unique name that you specify to match with the URI in RTP-Info header of the RTSP message.
string must be an alpha and/or numeric string of 1 through 127 characters in length. string allows punctuation characters and it does not include the “host” portion.

Usage
Use this command to specify a rule definition to analyze user traffic matching the “URI” field in the RTP-Info header of the RTSP response for a PLAY request.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTP-URI string of rtsp://www.foo.com in RTP-info header of RTSP packet:

```
rtsp rtp-uri = rtsp://www.foo.com
```
rtsp session-id

This command defines a rule definition to analyze and charge user traffic based on the RTSP session ID.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp session-id [ case-sensitive ] operator session_id

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • ! =: does not equal
  • ! contains: does not contain
  • ! ends-with: does not end with
  • ! starts-with: does not start with
  • =: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

session_id
An unique session Id for the RTSP user.
session_id must be an alpha and/or numeric string of 1 through 127 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on an RTSP session ID.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP session ID of 0123abc100:
\texttt{rtsp session-id} = 0123abc100
rtsp session-length

This command defines a rule definition to analyze and charge user traffic based on the RTSP session length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp session-length operator session_length

- no
Removes the specified rule definition.

- operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

  - !=: does not equal
  - <=: less than or equals
  - ==: equals
  - >=: greater than or equals

- session_length
Specifies the RTSP session length, in bytes, for this rule definition.
session_length must be an integer from 1 through 40000000.

Usage
Use this command to specify a rule definition to analyze, compare, or match the total length of RTSP session. The session-length is calculated by adding together the IP payloads (i.e., starting after the IP header) of all relevant packets.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP session length of 3000 bytes:

```
rtsp session-length = 3000
```
rtsp state

This command defines a rule definition to analyze and charge user traffic based on RTSP state.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp state operator state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- !=: does not equal
- ==: equals

state
Specifies the RTSP state for this rule definition. state must be one of the following:

- end
- init
- open
- play
- ready
- record

Usage
Use this command to specify a rule definition to analyze user traffic based on an RTSP state.

Example
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP in state of init:

rtsp state = init
rtsp uri

This command defines a rule definition to analyze and charge user traffic based on the uniform resource identifier (URI) in RTSP message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] rtsp uri [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!`: does not equal
  - `!=contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  A unique name that you specify to match with the URI in RTSP header.
  `string` must be an alpha and/or numeric string of 1 through 127 characters in length. `string` allows punctuation characters and it does not include the “host” portion.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a URI in RTSP header.

**Example**
The following command creates an RTSP rule definition for analyzing user traffic using an RTSP URI string of
rtsp://www..example.com:554/twister/audiotrack:

```
rtsp uri = rtsp://www.example.com:554/twister/audiotrack
```
rtsp uri sub-part

This command defines a rule definition to analyze and charge user traffic by parsing sub-parts of the URI in an RTSP request message.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] rtsp uri sub-part { { absolute-path | host | query } [ case-sensitive ]
operator string | port { port_operator port_value | { range | !range
} range_front | range_to } }
```

- **no**
Removes the specified rule definition.

- **absolute-path**
Specifies the absolute path matching criteria to RTSP URI in an RTSP request message.

- **host**
Specifies the host name matching criteria to RTSP URI in an RTSP request message.

- **query**
Specifies the query string matching criteria to RTSP URI in an RTSP request message.

- **case-sensitive**
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
Specifies how to logically match the information in the analyzed field.

  - operator must be one of the following:
    - `!=` does not equal
    - `!contains`: does not contain
    - `!ends-with`: does not end with
    - `!starts-with`: does not start with
    - `=`: equals
    - `contains`: contains
    - `ends-with`: ends with
    - `starts-with`: starts with
string
A unique absolute path/host name or query string that you specify to match with the URI in RTSP header. string must be an alpha and/or numeric string of 1 through 127 characters in length. string allows punctuation characters and it does not include the “host” portion.

port
Specifies the port related matching for RTSP URI in an RTSP request message.

port_operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- <=: less than or equals
- ==: equals
- >=: greater than or equals

port_value
Specifies the RTSP port number used for matching with port rule in RTSP flow. port_value must be an integer from 0 through 65535.

{ range | !range } range_from to range_to
Enables or disables the range criteria for RTSP flow ports.
range: Enables the range criteria for RTSP flow ports.
!range: Disables the range criteria for RTSP flow ports.
range_from: Specifies the start of range of RTSP flow ports and value must be an integer from 0 through 65535 but less than or equal to range_to.
range_to: Specifies the end of range of RTSP flow ports and value must be an integer from 0 through 65535 but more than or equal to range_from.

Usage
Use this command to specify a rule definition to analyze user traffic based on a URI sub parts like host, absolute path, port, and query in RTSP request message.

Example
The following command creates an RTSP URI sub part rule definition to analyze user traffic using an RTSP URI port number between 1023 and 1068:

    rtsp uri sub-part port range 1023 to 1068
rtsp user-agent

This command defines a rule definition to analyze and charge user traffic matching ‘user-agent’ field in RTSP header.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] rtsp user-agent [ case-sensitive ] operator user_agent

- no
  Removes the specified rule definition.

- case-sensitive
  Default: Disabled
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- operator
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  • !=: does not equal
  • !contains: does not contain
  • !ends-with: does not end with
  • !starts-with: does not start with
  • :=: equals
  • contains: contains
  • ends-with: ends with
  • starts-with: starts with

- user_agent
  Specifies the user agent in RTSP header for this rule definition.
  user_agent must be an alpha and/or numeric string of 1 through 127 characters in length.

Usage
Use this command to specify a rule definition to analyze user agent field in RTSP header.

Example
The following command creates a rule definition for analyzing user traffic using content as test in “user-agent” field of RTSP header:
rtsp user-agent = test
**rule-application**

This command specifies the application rule for the rule definition.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
rule-application { charging | post-processing | routing }

no rule-application
```

- **no**
  Removes the previous rule application configuration.

- **routing**
  Default: Disabled
  Specifies that this rule definition only be used for routing purposes.
  Up to 256 rule definitions can be defined for routing in an Active Charging Service.

- **post-processing**

  **Important:** The `post-processing` keyword is only available in StarOS 8.3 and later.

  Specifies that this rule definition only be used for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.

- **charging**
  Default: Enabled
  Specifies that this rule definition only be used for charging purposes.
  Up to 2048 rule definitions can be defined for charging application in an Active Charging Service.

**Usage**

Use this command to assign a rule application to a rule definition.
If, when configuring a ruledef, the rule-application is not specified, by default the system configures the ruledef as a charging ruledef.

**Example**
The following command assigns a rule application of charging to the current rule definition:

```plaintext
rule-application charging
```
The following commands define rules for analyzing traffic based on Session Description Protocol (SDP):
**sdp any-match**

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for SDP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sdp any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `! =`: does not equal
  - `= =`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the SDP any match status.

**Example**
The following command defines an any match rule definition for analyzing SDP user traffic as `TRUE`:

```
sdp any-match = TRUE
```
sdp connection-ip-address

This command defines a rule definition to analyze and charge user traffic based on SDP connection IP address.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] sdp connection-ip-address operator ip_address

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- !=: does not equal
- ==: equals

ip_address
The connection IP address expressed in IPv4 dotted decimal notation.

Usage
Use this command to specify a rule definition to analyze user traffic based on the SDP connection-ip-address.

Example
The following command defines a rule definition for analyzing sdp user traffic using an SDP connection-ip-address of 1.1.1.1:

sdp connection-ip-address = 1.1.1.1
sdp media-audio-port

This command defines a rule definition to analyze and charge user traffic based on SDP media-audio-port.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
[ no ] sdp media-audio-port operator port
```

- **no**  
  Removes the specified rule definition.

- **operator**  
  Specifies how to logically match the information in the analyzed field.  
  **operator** must be one of the following:
  - 
    - !: does not equal
  - =: equals

- **port**  
  Specifies the port number for this rule definition.  
  **port** must be an integer from 0 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an SDP media-audio-port.

**Example**

The following command creates an SDP rule definition for analyzing user traffic using SDP media audio port 10:

```
sdp media-audio-port = 10
```
Ruledef Configuration Mode Commands

sdp media-video-port

This command defines a rule definition to analyze and charge user traffic based on SDP media-video-port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] sdp media-video-port operator port

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !=: does not equal
- ==: equals

port
Specifies the port number for this rule definition.
port must be an integer from 0 through 65535.

Usage
Use this command to specify a rule definition to analyze user traffic based on an SDP media-video-port.

Example
The following command creates an SDP rule definition for analyzing user traffic using SDP media video port 10:

sdp media-video-port = 10
**sdp uplink**

This command defines a rule definition to analyze and charge user traffic based on SDP uplink.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sdp uplink operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **condition**
  Specifies the condition for this rule definition. `condition` must be one of the following:
  - `FALSE`: is not uplink
  - `TRUE`: is uplink

**Usage**

Use this command to specify a rule definition to analyze user traffic based on whether the SDP traffic is uplink or not uplink.

**Example**

The following command defines a rule definition for analyzing SDP user traffic using an SDP uplink status is not equal to `FALSE`:

```
sdp uplink != FALSE
```
The following commands define rules for analyzing traffic based on Secure-HTTP:
secure-http any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for Secure HTTP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] secure-http any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `! =`: does not equal
  - `= =`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

Usage
Use this command to specify a rule definition to analyze user traffic based on the HTTP any match status.

Example
The following command creates an HTTPS rule definition for analyzing user traffic using an HTTPS any match status of `FALSE`:

```
secure-http any-match = FALSE
```
secure-http uplink

This command defines a rule definition to analyze and charge user traffic based on Secure-HTTP uplink.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] secure-http uplink operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `FALSE`: is not uplink
  - `TRUE`: is uplink

**Usage**
Use this command to specify a rule definition to analyze user traffic based on whether the HTTPS traffic is uplink or not uplink.

**Example**
The following command defines a rule definition for analyzing HTTPS user traffic using an HTTPS uplink status is not equal to `FALSE`:

```
secure-http uplink ! = FALSE
```
The following commands define rules for analyzing traffic based on Session Initiation Protocol (SIP):
sip any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for SIP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] sip any-match operator condition

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator must be one of the following:*
  - • !=: does not equal
  - • ==: equals

- **condition**
  Specifies the condition for this rule definition.
  *condition must be one of the following:*
  - • FALSE
  - • TRUE

Usage

Use this command to specify a rule definition to analyze user traffic based on the SIP any match status.

Example

The following command defines an any match rule definition for analyzing SIP user traffic:

```
sip any-match = TRUE
```
**sip call-id**

This command defines a rule definition to analyze and charge user traffic based on the SIP call ID.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sip call-id [ case-sensitive ] operator call-id
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **call-id**
  `call-id` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**
Use this command to specify a SIP call ID rule definition to analyze user traffic based on a SIP call ID.

**Example**
The following command creates a rule definition for analyzing user traffic using a SIP call ID of `test`:

```
sip call-id = test
```
sip call-id
**sip content length**

This command defines a rule definition to analyze and charge user traffic based on the SIP content length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sip content length operator content_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
    - `!=`: does not equal
    - `<=`: less than or equals
    - `==`: equals
    - `>=`: greater than or equals

- **content_length**
  Specifies the SIP content length for this rule definition. `content_length` must be an integer from 0 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a SIP content length.

**Example**

The following command creates a SIP rule definition for analyzing user traffic using a SIP content length of **10000**:

```
sip content length = 10000
```
sip content type

This command defines a rule definition to analyze and charge user traffic based on the SIP content type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sip content type [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  Specifies content type is used in this rule definition.
  `string` must be an alpha and/or numeric string of 1 through 127 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a SIP content type.

**Example**

The following command creates a SIP rule definition for analyzing user traffic using a SIP content type as `download_string`. 

```
```


```
sip content type = download_string
```
sip from

This command defines a rule definition to analyze and charge user traffic based on the SIP from.

Product  
All

Privilege  
Security Administrator, Administrator

Syntax

[ no ] sip from [ case-sensitive ] operator string

no

Removes the specified rule definition.

case-sensitive

Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator

Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- !: does not equal
- !=: contains: does not contain
- !=ends-with: does not end with
- !=starts-with: does not start with
- =: equals
- contains: contains
- ends-with: ends with
- starts-with: starts with

string

Specifies the string for this rule definition. string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on a SIP from value.

Example

The following command creates a SIP rule definition for analyzing user traffic containing a SIP from value of test1:

```
sip from contains test1
## sip previous-state

This command defines a rule definition to analyze and charge user traffic based on the SIP previous state.

### Product
All

### Privilege
Security Administrator, Administrator

### Syntax

```
[ no ] sip previous-state operator previous_state
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
<th>Removes the specified rule definition.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>operator</strong></th>
<th>Specifies how to logically match the information in the analyzed field. <strong>operator</strong> must be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>!=</code></td>
<td>does not equal</td>
</tr>
<tr>
<td><code>=</code></td>
<td>equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>previous_state</strong></th>
<th>Specifies the SIP previous state for this rule definition. <strong>previous_state</strong> must be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>init</code></td>
<td></td>
</tr>
<tr>
<td><code>provisional-response</code></td>
<td></td>
</tr>
<tr>
<td><code>request-sent</code></td>
<td></td>
</tr>
<tr>
<td><code>response-fail</code></td>
<td></td>
</tr>
<tr>
<td><code>response-ok</code></td>
<td></td>
</tr>
</tbody>
</table>

### Usage

Use this command to specify a rule definition to analyze user traffic based on a SIP previous state.

### Example

The following command creates a SIP rule definition for analyzing user traffic using a SIP previous state of `request-sent`:

```
sip previous-state = request-sent
```
**sip reply code**

This command defines a rule definition to analyze and charge user traffic based on the SIP reply code.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sip reply code operator return_code
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **return_code**
  Specifies the SIP return code for this rule definition. `return_code` must be an integer from 100 through 699.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a SIP reply code.

**Example**

The following command creates a SIP rule definition for analyzing user traffic using a SIP reply code of 150:

```
sip reply code = 150
```
sip request method

This command defines a rule definition to analyze and charge user traffic based on the SIP request method.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] sip request method operator method

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• ==: equals

method
Specifies the SIP method for this rule definition.
method must be one of the following:
• ack
• bye
• cancel
• invite
• options
• register

Usage
Use this command to specify a rule definition to analyze user traffic based on SIP method.

Example
The following command defines a rule definition for analyzing SIP user traffic using SIP request method bye:

    sip request method = bye
sip request packet

This command defines a rule definition to analyze and charge user traffic based on the SIP request packet.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] sip request packet operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
- \( = \): equals
- \( \neq \): not equals

condition
The type of SIP packet is request. condition must be one of the following:
- \( \text{FALSE} \): is a response
- \( \text{TRUE} \): is a request

Usage
Use this command to specify a rule definition to analyze user traffic based on the SIP request packet.

Example
The following command defines a rule definition for analyzing SIP user traffic using a SIP request packet is equals to request:

sip request packet = TRUE
**sip state**

This command defines a rule definition to analyze and charge user traffic based on the SIP state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sip state operator state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **state**
  Specifies the sip state for this rule definition. `state` must be one of the following:
  - `ack-received`
  - `provisional-response`
  - `request-sent`
  - `response-fail`
  - `response-ok`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a SIP state.

**Example**

The following command creates a SIP rule definition for analyzing user traffic using a SIP state of `request-sent`:

```
sip state = request-sent
```
This command defines a rule definition to analyze and charge user traffic based on the “to” field of SIP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] sip to [ case-sensitive ] operator sip_to_field
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!=contains`: does not contain
  - `!=ends-with`: does not end with
  - `!=starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **sip_to_field**
  Specifies the SIP to value for this rule definition.
  `sip_to_field` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a SIP to value.

**Example**
The following command creates a SIP rule definition for analyzing user traffic containing a SIP to value of `test1`:
sip to contains test1
sip uri

This command defines a rule definition to analyze and charge user traffic based on the SIP URI.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] sip uri [ sub-part { headers | host | parameters | port | userinfo } ] [ case-sensitive ] operator string
```

**no**
Removes the specified rule definition.

**sub-part { headers | host | parameters | port | userinfo }**
This is an optional keyword that defines what sub-part of a SIP URI to check.
- **headers**: Apply the rule to SIP URI header field.
- **host**: Apply the rule the SIP URI host field.
- **parameters**: Apply the rule to the SIP URI parameters field.
- **port**: Apply the rule to the SIP URI port field.
- **userinfo**: Apply the rule to the SIP URI userinfo field.

**case-sensitive**
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

**operator**
Specifies how to logically match the information in the analyzed field. **operator** must be one of the following:
- `!=`: does not equal
- `!contains`: does not contain
- `!ends-with`: does not end with
- `!starts-with`: does not start with
- `=`: equals
- `contains`: contains
- `ends-with`: ends with
- `starts-with`: starts with

The string for sub-part keyword **port** must be an integer and requires different operators. Use the following operators with the **port** keyword:
- `!=`: does not equal
- `<=`: is less than
Ruledef Configuration Mode Commands

### sip uri

- `•=`: equals
- `•>:=` : is greater than

**string**

A unique name that you specify for a SIP URI.

`string` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

The string for sub-part keyword `port` must be an integer from 0 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a SIP URI.

**Example**

The following command creates a SIP rule definition for analyzing user traffic using a SIP URI string:

```
sip uri = sip:192.168.1.51:5060
```

```
sip uri = sip:nnnnn@host:5060;user=phone
```
smtp

The following defines common syntax block options. These options appear in similar commands and are detailed here for easy reference.
smtp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for SMTP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] smtp any-match [ operator ] [ condition ]
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `! =`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition.
  *condition* must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify an any match rule definition on analyzing user traffic based on the SMTP analyzed status.

**Example**

The following command defines an any match rule definition for analyzing SMTP user traffic:

```
smtp any-match = TRUE
```
smtp command arguments

This command defines a rule definition to analyze and charge user traffic based on the SMTP command arguments.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] smtp command arguments [ case-sensitive ] operator argument
```

- **no**
  
  Removes the specified rule definition.

- **case-sensitive**
  
  Default: Disabled.
  
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  
  Specifies how to logically match the information in the analyzed field.
  
  *operator* must be one of the following:
  
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **argument**
  
  A unique value that you specify to use for the command argument.
  
  *argument* must be an alpha and/or numeric string of 1 through 63 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an SMTP command argument.

**Example**

The following command defines a rule definition for analyzing SMTP user traffic using a command argument of `test`: 
smtp command arguments = test
smtp command id

This command defines a rule definition to analyze and charge user traffic based on the SMTP command ID.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] smtp command id operator command_id
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `==`: equals
  - `=>`: greater than or equals

- **command_id**
  A unique value that you specify to use for the command argument.
  `command_id` must be an integer from 0 through 10.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an SMTP command ID.

**Example**

The following command defines a rule definition for analyzing POP3 user traffic using a command ID of 8:

```
smtp command id = 8
```
smtp command name

This command defines a rule definition to analyze and charge user traffic based on the SMTP command name.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] smtp command name operator command_name
```

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- `!=`: does not equal
- `==`: equals

command_name
command_name must be one of the following:
- `bdat`
- `data`
- `ehlo`
- `expn`
- `helo`
- `mail-from`
- `noop`
- `quit`
- `rcpt-to`
- `rset`
- `vrfy`

Usage
Use this command to specify a rule definition to analyze user traffic based on an SMTP command name.

Example
The following command defines a rule definition for analyzing SMTP user traffic using a command name of `data`:
smtp command name = data
smtp mail-size

This command defines a rule definition to analyze and charge user traffic based on the SMTP mail size.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] smtp mail-size \{ operator mail_size \} \{ \{ range | !range \} \}
```

**no**
Removes the specified rule definition.

**operator**
Specifies how to logically match the information in the analyzed field. 
**operator** must be one of the following:
- `!=`: does not equal
- `<=`: less than or equals
- `==`: equals
- `>=`: greater than or equals

**mail_size**
Specifies the mail size, in bytes, for this rule definition.
**mail_size** must be an integer from 1 through 40000000.

**{ range | !range } range_from to range_to**
Enables or disables the range criteria.
**range**: Enables the range criteria.
**!range**: Disables the range criteria.
**range_from**: Specifies the start of range, and must be an integer from 1 through 40000000.
**range_to**: Specifies the end range. **range_to** must be an integer from 1 through 40000000, and must be greater than **range_from**

Usage
Use this command to specify a rule definition to analyze user traffic based on SMTP mail size.

Example
The following command defines a rule definition for analyzing SMTP user traffic using a mail size of 40000:

```
smtp mail-size = 40000
```
smtp pdu-length

This command defines a rule definition to analyze and charge user traffic based on the SMTP protocol data unit (PDU) length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] smtp pdu-length \{ operator pdu_length | \{ range | !range \} range_from to range_to \}
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!`: does not equal
  - `<<=`: less than or equals
  - `=`: equals
  - `><=`: greater than or equals

- **pdu_length**
  Specifies the SMTP PDU length, in bytes, for this rule definition. `pdu_length` must be an integer from 1 through 65535.

- **\{ range | !range \} range_from to range_to**
  Enables or disables the range criteria.
  - `range`: Enables the range criteria.
  - `!range`: Disables the range criteria.
  - `range_from`: Specifies the start of range, and must be an integer from 1 through 65535.
  - `range_to`: Specifies the end range. `range_to` must be an integer from 1 through 65535, and must be greater than `range_from`

Usage

Use this command to specify a rule definition to analyze user traffic based on an SMTP packet length.

Example

The following command defines a rule definition for analyzing SMTP user traffic using a PDU length of 1600 bytes:

```plaintext
smtp pdu-length = 1600
```
smtp pdu-length
smtp previous-state

This command defines a rule definition to analyze and charge user traffic based on the SMTP previous state.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] smtp previous-state operator pre_state

---

no
Removes the specified rule definition.

---

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !=: does not equal
- =: equals

---

pre_state
Specifies the previous state for this rule definition.
pre_state must be one of the following:
- close: closed state
- init: initialized state
- response-error: reply error state
- response-ok: response ok state
- waiting-for-response: waiting for response state

Usage
Use this command to specify a rule definition to analyze user traffic based on an SMTP previous state.

Example
The following command creates an SMTP rule definition for analyzing user traffic using an SMTP previous state of closed:

```
smtp previous-state = closed
```
smtp recipient

This command defines a rule definition to analyze and charge user traffic based on the SMTP recipient.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] smtp recipient [ case-sensitive ] operator argument
```

- **no**
  
  Removes the specified rule definition.

- **case-sensitive**
  
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **argument**
  
  A unique value that you specify to use for the response argument.
  `argument` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a recipient rule definition.

**Example**

The following command defines a rule definition for analyzing SMTP user traffic using a recipient of `test`:
smtp recipient = test
smtp reply arguments

This command defines a rule definition to analyze and charge user traffic based on the SMTP reply argument.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] smtp reply arguments[ case-sensitive ]operator argument

- no
  Removes the specified rule definition.

- case-sensitive
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- operator
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  - !=: does not equal
  - !contains: does not contain
  - !ends-with: does not end with
  - !starts-with: does not start with
  - =: equals
  - contains: contains
  - ends-with: ends with
  - starts-with: starts with

- argument
  Specifies the string for this rule definition.
  argument must be an alpha and/or numeric string of 1 through 63 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on an SMTP reply argument.

Example

The following command creates an SMTP reply argument rule definition for analyzing user traffic using a reply argument of test:
smtp reply arguments = test
smtp reply id

This command defines a rule definition to analyze and charge user traffic based on the SMTP reply ID.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] smtp reply id operator reply_id

---

no

Removes the specified rule definition.

---

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- !: does not equal
- := equals

---

reply_id

Specifies the reply ID for this rule definition.
reply_id must be one of the following:

- 0: +NO reply
- 1: +OK reply
- 2: -ERR reply

---

Usage

Use this command to specify a rule definition to analyze user traffic based on an SMTP reply ID.

Example

The following command defines a rule definition for analyzing SMTP user traffic using a reply ID of 2:

```
smtp reply id = 2
```
**smtp reply status**

This command defines a rule definition to analyze and charge user traffic based on the SMTP reply status.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] smtp reply status operator reply_status
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **reply_status**
  Specifies the response ID for this rule definition.
  `reply_status` must be one of the following:
  - `+OK`: response OK
  - `-ERR`: response error

**Usage**

Use this command to specify a rule definition to analyze user traffic based on an SMTP reply status.

**Example**

The following command defines a rule definition for analyzing SMTP user traffic using a reply status of `+OK`:

```plaintext
smtp reply status = +OK
```
smtp sender

This command defines a rule definition to analyze and charge user traffic based on the SMTP sender.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] smtp sender [ case-sensitive ] operator sender
```

**no**
Removes the specified rule definition.

**case-sensitive**
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

**operator**
Specifies how to logically match the information in the analyzed field.
`operator` must be one of the following:
- `!=`: does not equal
- `!contains`: does not contain
- `!ends-with`: does not end with
- `!starts-with`: does not start with
- `=`: equals
- `contains`: contains
- `ends-with`: ends with
- `starts-with`: starts with

**sender**
Specifies the session length used for this rule definition.
`sentry` must be an alpha/or numeric string of 1 through 127 characters in length.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the SMTP session length.

**Example**
The following command creates an SMTP rule definition for analyzing user traffic using an SMTP sender of `test`:

```
smtp sender = test
```
smtp session-length

This command defines a rule definition to analyze and charge user traffic based on the SMTP session-length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[
\text{[ no ] smtp session-length } \text{ operator } \text{ sess.length } \text{ range | !range range_from to range_to}
\]

- `no` Removes the specified rule definition.
- `operator` Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals
- `sess.length` Specifies the session length for this rule definition. `sess.length` must be an integer from 1 through 40000000.
- `{ range | !range } range_from to range_to` Enables or disables the range criteria.
  - `range`: Enables the range criteria.
  - `!range`: Disables the range criteria.
  - `range_from`: Specifies the start of range, and must be an integer from 1 through 40000000.
  - `range_to`: Specifies the end range. `range_to` must be an integer from 1 through 40000000, and must be greater than `range_from`

Usage
Use this command to specify a rule definition to analyze user traffic based on the SMTP session length.

Example
The following command creates an SMTP rule definition for analyzing user traffic using an SMTP session length of 4000000:

```
smtp session-length = 4000000
```
smtp state

This command defines a rule definition to analyze and charge user traffic using SMTP state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] smtp state operator state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **state**
  Specifies the SMTP state for this rule definition. `state` must be one of the following:
  - `close`: closed state
  - `init`: initialized state
  - `response-error`: response of error state
  - `response-ok`: response of ok state
  - `waiting-for-response`: waiting for response state

**Usage**

Use this command to specify a rule definition to analyze user traffic based on SMTP state.

**Example**

The following command creates an SMTP rule definition for analyzing user traffic using an SMTP state of `close`:

```
smtp state = close
```
tcp

The following commands define rules for analyzing traffic based on Transmission Control Protocol (TCP):
tcp analyzed out-of-order

This command specifies counting/charging of all TCP out-of-order packets that are received and buffered at ACSMgr/SessMgr due to non receipt of earlier packet(s) in sequence.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp analyzed out-of-order operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !=: does not equal
- ==: equals

condition
Specifies the condition for this rule definition.
condition must be one of the following:
- FALSE: not analyzed
- TRUE: analyzed

Usage
This command is used to set the status flag to ‘analyzed’ or ‘not analyzed’ for all TCP packets received at the ACSMgr/SessMgr prior to their earlier packets.
When a packet reaches ACSMgr/SessMgr prior to earlier packet(s), particular packet with subsequent packets are buffered at ACSMgr/SessMgr as TCP out-of-order packets and ACSMgr/SessMgr waits for missing packet(s) till time-out duration expires. If the packet(s) with the missing sequence number(s) arrives within time-out duration, all buffered packets with correct sequence will be presented to upper layers (HTTP etc.) for analysis; otherwise buffered TCP out-of-order packets will be sent to charging with analysis done flag at TCP/IP layer only.
If this command is enabled the TCP out-of-order packets marked and sent to TCP analyzer as analyzed for charging action otherwise discarded.

Example
The following command sets to analyze TCP out-of-order packets:

tcp analyzed out-of-order = TRUE
tcp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for TCP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] tcp any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  - `!`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition.
  - `FALSE`: not analyzed
  - `TRUE`: analyzed

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the tcp any match status.

**Example**
The following command defines an any match rule definition for analyzing TCP user traffic:

```
tcp any-match = TRUE
```
tcp connection-initiator

This command defines a rule definition to analyze and charge user traffic based on the TCP connection initiator.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp connection-initiator operator subscriber

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. "operator" must be one of the following:

- !=: does not equal
- =: equals

subscriber
Specifies that the connection is being initiated by the subscriber.

Usage
Use this command to specify a rule definition to analyze user traffic based on the TCP connection initiator and to allow the operator to differentiate between connection initiated by subscriber or the subscriber is acting as a TCS (Transaction Control Server) server.

Example
The following command creates TCP rule definition for analyzing user traffic using an TCP connection initiator as subscriber:

tcp connection-initiator = subscriber
tcp downlink

This command defines a rule definition to analyze and charge user traffic matching the direction of TCP packets to downlink (to subscriber).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp downlink operator condition

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Removes the specified rule definition.

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
</table>
| Specifies how to logically match the information in the analyzed field.
| operator must be one of the following:
| • ! =: does not equal
| • =: equals

<table>
<thead>
<tr>
<th>condition</th>
</tr>
</thead>
</table>
| Specifies the condition for this rule definition.
| condition must be one of the following:
| • FALSE
| • TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the TCP packet direction as downlink.

Example
The following command creates TCP rule definition for analyzing user traffic using an TCP packet direction to downlink (to subscriber):

```
tcp downlink = TRUE
```
**tcp dst-port**

This command defines a rule definition to analyze and charge user traffic based on destination TCP port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] tcp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the port number.
  *operator must be one of the following:*
  *!=:* Does not equal
  *<=:* Less than or equals
  *=:* Equals
  *>=:* Greater than or equals

- **port_number**
  Specifies the port number to match.
  *port_number must be an integer from 1 through 65535.*

- **range | !range**
  Specifies the range criteria:
  *!range: Not in the range
  *range: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the range of destination TCP ports.
  *start_range must be an integer from 1 through 65535.*
  *end_range must be an integer from 1 through 65535, and must be greater than start_range*

- **port-map port_map**
  Specifies the port map for the port range.
  *port_map must be a string of 1 through 63 characters in length.*

**Usage**
Use this command to specify a rule definition to analyze user traffic based on destination TCP port.

Example
The following command creates a TCP rule definition for analyzing user traffic matching destination port for TCP as 10:

```
tcp dst-port = 10
```
tcp duplicate

This command defines a rule definition to analyze and charge user traffic using duplicate TCP packet.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] tcp duplicate operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `FALSE`: not duplicated/retransmitted
  - `TRUE`: duplicated/retransmitted

**Usage**

Use this command to specify a duplicate rule definition for analyzing user traffic.

**Example**
The following command defines a duplicate rule definition with a value of `TRUE`:

```
tcp duplicate = TRUE
```
**tcp either-port**

This command defines a rule definition to analyze and charge user traffic using either (destination or source) TCP port.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] tcp either-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the port number.
  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `<=`: Less than or equals
    - `==`: Equals
    - `>=`: Greater than or equals

- **port_number**
  - Specifies the port number to match.
  - **port_number** must be an integer from 1 through 65535.

- **range | !range**
  - Specifies the range criteria:
    - `!range`: Not in the range
    - `range`: In the range

- **start_range to end_range**
  - Specifies the starting and ending port numbers for the port range.
  - **start_range** must be an integer from 1 through 65535.
  - **end_range** must be an integer from 1 through 65535, and must be greater than **start_range**.

- **port-map port_map**
  - Specifies the port-map for the port range.
  - **port_map** must be a string of 1 through 63 characters in length.

**Usage**

---

**Cisco ASR 5000 Series Command Line Interface Reference**

4762
Use this command to specify a rule definition to analyze user traffic based on either TCP port.

**Example**
The following command creates a TCP rule definition for analyzing user traffic matching destination or source port for TCP as 10:

```
tcp either-port = 10
```
tcp error

This command defines a rule definition to identify any erroneous TCP packets.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

\[
\begin{array}{l}
\text{[ no ] tcp error operator condition} \\
\end{array}
\]

- **no**
  - Removes the specified rule definition.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - `operator` must be one of the following:
    - `!=`: does not equal
    - `==`: equals

- **condition**
  - Specifies the condition for this rule definition.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage**

Use this command to specify a rule definition to identify any erroneous TCP packets.

**Example**

The following command creates a TCP rule definition for identifying an erroneous TCP packet:

```plaintext
tcp error = TRUE
```
tcp flag

This command defines a rule definition to analyze and charge user traffic based on the TCP flag.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```markdown
[ no ] tcp flag operator value
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• !contains: does not contain</td>
</tr>
<tr>
<td>• contains: contains</td>
</tr>
<tr>
<td>• !=: does not equal</td>
</tr>
<tr>
<td>• =: equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The value of the specified field.</td>
</tr>
<tr>
<td>value must be one of the following:</td>
</tr>
<tr>
<td>• ack: TCP FLAG ACK</td>
</tr>
<tr>
<td>• fin: TCP FLAG FIN</td>
</tr>
<tr>
<td>• push: TCP FLAG PUSH</td>
</tr>
<tr>
<td>• reset: TCP FLAG RESET</td>
</tr>
<tr>
<td>• syn: TCP FLAG SYN</td>
</tr>
</tbody>
</table>

Usage

Use this command to specify a flag rule definition for analyzing user traffic.

Example

The following command defines a flag rule definition with a value of reset:

```bash
tcp flag = reset
```
tcp initial-handshake-lost

This command defines a rule definition to identify a TCP flow where the initial handshake was not seen.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] tcp initial-handshake-lost operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition. `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**
Use this command to specify a rule definition to identify a TCP flow where the initial handshake was not seen.

**Example**
The following command creates a TCP rule definition for identifying a TCP flow where the initial handshake was not seen:

```
tcp initial-handshake-lost = TRUE
```
tcp payload

This command defines a rule definition to analyze and charge user traffic based on Hex/ASCII string content in payload protocol-signature field of TCP payload.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp payload starts-with { hex-signature hex_string | string-signature string }

no
Removes the specified rule definition.

hex-signature hex_string
Specifies hexadecimal protocol signature in payload field. 
hex_string must be a dash-delimited list of hex data of size smaller than 32.

string-signature string
Specifies protocol signature in payload field. 
string must be a string of 1 through 32 characters in length.

Usage
Use this command to define a rule definition to analyze user traffic based on a match for Hex/ASCII string content in payload protocol-signature field.

Example
The following command creates a TCP rule definition to identify user traffic using TCP protocol signature as tcp1:

tcp payload starts-with string-signature tcp1
tcp payload-length

This command defines a rule definition to analyze and charge user traffic based on the TCP payload length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp payload-length operator payload_length

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. 
operator must be one of the following:

- !=: does not equal
- <=: less than or equals
- ==: equals
- >=: greater than or equals

payload_length
Specifies the tcp payload length for this rule definition. 
payload_length must be an integer from 0 through 40000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on a TCP payload length.

Example
The following command creates a TCP rule definition for analyzing user traffic using a TCP payload length of 10000:

```
tcp payload-length = 10000
```
tcp previous-state

This command defines a rule definition to analyze and charge user traffic using previous state of TCP packet.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp previous-state operator previous_state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
• !=: does not equal
• ==: equals

previous_state
Specifies the TCP previous state for this rule definition. previous_state must be one of the following:
• close
• close-wait
• closing
• established
• fin-wait1
• fin-wait2
• last-ack
• listen
• syn-received
• syn-sent
• time-wait

Usage
Use this command to specify a rule definition to analyze user traffic based on a TCP previous state.

Example
The following command creates a TCP rule definition for analyzing user traffic using a TCP previous state of time-wait:
tcp previous-state = time-wait
tcp session-length

This command defines a rule definition to analyze and charge user traffic using TCP session length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• <=: less than or equals
• ==: equals
• >=: greater than or equals

sess_length
Specifies the TCP session length, in bytes, for this rule definition.
sess_length must be an integer from 0 through 4000000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on the TCP session length.

Example
The following command creates a TCP rule definition for analyzing user traffic using a TCP session length of 2000 bytes:

tcp session-length = 2000
**tcp src-port**

This command defines a rule definition to analyze and charge user traffic based on source TCP port.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] tcp src-port { operator port_number | !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the port number.
  `operator` must be one of the following:
  - `!`: does not equal
  - `<`: Less than or equals
  - `=`: equals
  - `>`: greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 through 65535.

- **range | !range**
  Specifies the range criteria:
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  `start_range` must be an integer from 1 through 65535.
  `end_range` must be an integer from 1 through 65535, and must be greater than `start_range`.

- **port-map port_map**
  Specifies the port map for the port range.
  `port_map` must be a string of 1 through 63 characters in length.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on source TCP port.

**Example**

The following command creates a TCP rule definition for analyzing user traffic matching source port for TCP as 10:

```
tcp src-port = 10
```
tcp state

This command defines a rule definition to analyze and charge user traffic using current state of TCP packet.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] tcp state operator state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **state**
  Specifies the TCP state for this rule definition.
  `state` must be one of the following:
  - `close`
  - `close-wait`
  - `closing`
  - `established`
  - `fin-wait1`
  - `fin-wait2`
  - `last-ack`
  - `listen`
  - `syn-received`
  - `syn-sent`
  - `time-wait`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a TCP state.

**Example**

The following command creates a TCP rule definition for analyzing user traffic using a TCP state of `close`:
tcp state = close
tcp uplink

This command defines a rule definition to analyze and charge user traffic matching the direction of TCP packets to uplink (from subscriber).

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] tcp uplink operator condition

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• ! =: does not equal</td>
</tr>
<tr>
<td>• =: equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the condition for this rule definition.</td>
</tr>
<tr>
<td>condition must be one of the following:</td>
</tr>
<tr>
<td>• FALSE</td>
</tr>
<tr>
<td>• TRUE</td>
</tr>
</tbody>
</table>

Usage
Use this command to specify a rule definition to analyze user traffic based on the TCP packet direction as uplink.

Example
The following command creates TCP rule definition for analyzing user traffic using an TCP packet direction to uplink (from subscriber):

tcp uplink = TRUE
udp

The following commands define rules for analyzing traffic based on User Datagram Protocol (UDP):

```
udp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for UDP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] udp any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition. 
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the UDP analyzed status.

**Example**

The following command defines an any match rule definition for analyzing UDP user traffic:

```
udp any-match = TRUE
```
udp downlink

This command defines a rule definition to analyze and charge user traffic based on the UDP downlink.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] udp downlink operator condition

no

Removes the specified rule definition.

operator

Specifies how to logically match the information in the analyzed field. 
operator must be one of the following:

• =: equals

condition

Specifies the condition for this rule definition.
condition must be one of the following: 

• FALSE
• TRUE

Usage

Use this command to specify a rule definition to analyze user traffic based on a UDP downlink condition.

Example

The following command creates a UDP rule definition for analyzing user traffic using UDP downlink condition TRUE

udp downlink = TRUE
udp dst-port

This command defines a rule definition to analyze and charge user traffic based on destination UDP port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```plaintext
{ [ no ] udp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

no
Removes the specified rule definition.

operator
Specifies how to logically match the port number.
operator must be one of the following:
- • !=: Does not equal
- • <=: Less than or equals
- • =: Equals
- • =>: Greater than or equals

port_number
Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range
Specifies the range criteria.
- • !range: Not in the range
- • range: In the range

start_range to end_range
Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535, and must be greater than start_range.

port-map port_map
Specifies the port map for the port range.
port_map must be a string of 1 through 63 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on destination UDP port.

Example
The following command creates a UDP rule definition for analyzing user traffic matching destination port for UDP as 10:

```
udp dst-port = 10
```
udp either-port

This command defines a rule definition to analyze and charge user traffic using either (destination or source) UDP port.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] udp either-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }

no
Removes the specified rule definition.

operator
Specifies how to logically match the port number.
operator must be one of the following:
• !: Does not equal
• <: Less than or equals
• =: Equals
• =>: Greater than or equals

port_number
Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range
Specifies the range criteria.
• !: Not in the range
• : In the range

start_range to end_range
Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535, and must be greater than start_range.

port-map port_map
Specifies the port map for the port range.
port_map must be a string of 1 through 63 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on either UDP port.

**Example**
The following command creates a UDP rule definition for analyzing user traffic matching destination or source port for UDP as 10:

```
udp either-port = 10
```
udp payload

This command defines rule to analyze and charge user traffic based on the match for Hex/ASCII string content in payload protocol-signature field in UDP payload.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] udp payload starts-with { hex-signature hex_string | string-signature string }

- no
  Removes the specified rule definition.

- hex-signature hex_string
  Specifies hexadecimal protocol signature in payload field. 
  hex_string must be a dash-delimited list of hex data of size smaller than 32.

- string-signature string
  Specifies protocol signature in payload field.
  string must be a string of 1 through 32 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on a match for Hex/ASCII string content in payload protocol-signature field.

Example
The following command creates a UDP rule definition for analyzing user traffic using a UDP protocol signature as udp1:

    udp payload starts-with string-signature udp1
udp src-port

This command defines a rule definition to analyze and charge user traffic based on source UDP port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] udp src-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the port number.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 through 65535.

- **!range | range**
  Specifies the range criteria.
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  `start_range` must be an integer from 1 through 65535.
  `end_range` must be an integer from 1 through 65535, and must be greater than `start_range`.

- **port-map port_map**
  Specifies the port map for the port range.
  `port_map` must be a string of 1 through 63 characters in length.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on source UDP port.

Example
The following command creates a UDP rule definition for analyzing user traffic matching source port for UDP as 10:

```
udp src-port = 10
```
udp uplink

This command defines a rule definition to analyze and charge user traffic based on the UDP uplink.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] udp uplink operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• =: equals

condition
Specifies the condition for this rule definition.
condition must be one of the following:
• FALSE
• TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on a UDP uplink condition.

Example
The following command creates a UDP rule definition for analyzing user traffic using UDP uplink condition TRUE:

udp uplink = TRUE
wsp

The following commands define rules for analyzing traffic based on Wireless Session Protocol (WSP):
wsp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for WSP.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] wsp any-match operator condition

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition. 
  `condition` must be one of the following:
  - **FALSE**
  - **TRUE**

Usage

Use this command to specify an any match WSP rule definition on analyzing user traffic.

Example
The following command defines an any match rule definition for analyzing WSP user traffic:

```
  wsp any-match = TRUE
```
**wsp content type**

This command defines a rule definition to analyze and charge user traffic based on the WSP content type.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] wsp content type [ case-sensitive ] operator content_type
```

- **no**
  - Removes the specified rule definition.

- **case-sensitive**
  - Default: Disabled.
  - This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - **operator** must be one of the following:
    - `!=`: does not equal
    - `!contains`: does not contain
    - `!ends-with`: does not end with
    - `!starts-with`: does not start with
    - `=`: equals
    - `contains`: contains
    - `ends-with`: ends with
    - `starts-with`: starts with

- **content_type**
  - **content_type** must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WSP content type.

**Example**

The following command creates a SIP rule definition for analyzing user traffic using a WSP content of `test`:

```
wsp content type = test
```
wsp downlink

This command defines a rule definition to analyze and charge user traffic using WSP downlink.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] wsp downlink operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !: does not equal
- =: equals

condition
Indicates the downlink (from the Mobile Node direction) status.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on a WSP downlink condition.

Example
The following command defines a rule definition for analyzing WSP user traffic based on the WSP downlink condition of TRUE:

wsp downlink = TRUE
**wsp first-request-packet**

This command defines a rule definition to analyze and charge user traffic based on the WSP first-request-packet.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wsp first-request-packet operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition. `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the WSP first request packet.

**Example**

The following command creates an WSP rule definition for analyzing user traffic testing for the first-request-packet equals **TRUE**:

```
wsp first-request-packet = TRUE
```
wsp host

This command defines a rule definition to analyze and charge user traffic using WSP host.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] wsp host [ case-sensitive ] operator host_name

- no
  Removes the specified rule definition.

- case-sensitive
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- operator
  Specifies how to logically match the information in the analyzed field.
  operator must be one of the following:
  - !=: does not equal
  - !contains: does not contain
  - !ends-with: does not end with
  - !starts-with: does not start with
  - =: equals
  - contains: contains
  - ends-with: ends with
  - starts-with: starts with

- host_name
  A unique name that you specify for the WSP host.
  host_name must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on a WSP host name.

Example

The following command creates a WSP rule definition for analyzing user traffic containing a WSP host of host1:
wsp host contains host1
wsp pdu-length

This command defines a rule definition to analyze and charge user traffic based on the WSP Protocol Data Unit (PDU) length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- ! =: does not equal
- < =: less than or equals
- = =: equals
- >=: greater than or equals

pdu_length
Specifies the WSP PDU length, in bytes, for this rule definition.
pdu_length must be an integer from 1 through 65535.

Usage
Use this command to specify a rule definition to analyze user traffic based on a WSP PDU length (header + payload) in bytes.

Example
The following command creates a WSP rule definition for analyzing user traffic using an WSP PDU length of 10000 bytes:

\[ \text{wsp pdu-length} = 10000 \]
wsp pdu-type

This command defines a rule definition to analyze and charge user traffic using WSP Protocol Data Unit (PDU) type.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] wsp pdu-type operator pdu_type

---

no

Removes the specified rule definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- !=: does not equal

- ==: equals

---

pdu_type

Specifies the WSP PDU type used for this rule definition.
pdu_type must be one of the following:

- confirmed push
- connect-reply
- connect-request
- data-fragment
- delete
- disconnect
- get
- head
- options
- post
- push
- put
- redirect
- reply
- resume
- suspend
- trace
**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WSP PDU type value.

**Example**

The following command creates a WSP rule definition for analyzing user traffic containing a WSP PDU type resume:

```
wsp pdu-type resume
```
wsp previous-state

This command defines a rule definition to analyze and charge user traffic using WSP previous state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] wsp previous-state operator previous_state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!:=` does not equal
  - `:=` equals

- **previous_state**
  Specifies the previous state for this rule definition.
  `previous_state` must be one of the following:
  - `init`
  - `response-error`
  - `response-ok`
  - `waiting-for-response`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a WSP previous state.

**Example**
The following command creates a WSP rule definition for analyzing user traffic using a WSP previous state of `response-ok`:

```plaintext
wsp previous-state = response-ok
```
**wsp reply code**

This command defines a rule definition to analyze and charge user traffic based on the WSP reply code.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
no
```

Removes the specified rule definition.

```plaintext
operator
```

Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:

- `!=`: does not equal
- `<=`: less than or equals
- `=`: equals
- `>=`: greater than or equals

```plaintext
return_code
```

Specifies the WSP return code for this rule definition. `return_code` must be an integer from 0 through 101.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WSP reply code.

**Example**
The following command creates a WSP rule definition for analyzing user traffic using a WSP reply code of 50:

```
wsp reply code = 50
```
**wsp session-length**

This command defines a rule definition to analyze and charge user traffic using WSP session length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
no

Removes the specified rule definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !: does not equal
- <=: less than equals
- =: equals
- >=: greater than equals

sess_length

Specifies the WSP session length, in bytes, for this rule definition.
sess_length must be an integer from 1 through 65535.
```

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the WSP session length.

**Example**
The following command creates a WSP rule definition for analyzing user traffic using a WSP session length of 2000 bytes:

```plaintext
wsp session-length = 2000
```
**wsp session-management**

This command defines a rule definition to analyze and charge user traffic based on WSP session management information.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] wsp session-management { previous-state | state } operator state
```

- **no**
  - Removes the specified rule definition.

- **previous-state**
  - Specifies WSP previous state information.

- **state**
  - Specifies WSP current state information.

- **operator**
  - Specifies how to logically match the information in the analyzed field. operator must be one of the following:
    - `!=`: does not equal
    - `=`: equals

- **state**
  - Specifies the WSP state.
  - For `previous-state`, state must be one of the following:
    - `connected`
    - `connecting`
    - `init`
    - `resuming`
    - `suspended`
  - For `state`, state must be one of the following:
    - `close`
    - `connected`
    - `connecting`
    - `init`
    - `resuming`
### Usage

Use this command to specify a rule definition to analyze user traffic based on WSP session management information.

### Example

The following command creates a WSP rule definition for analyzing user traffic based on WSP session-management current state of `connecting`:

```
wsp session-management state = connecting
```
wsp state

This command defines a rule definition to analyze and charge user traffic using WSP state.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[ \text{[ no ] \ wsp \ state} \ \text{operator} \ \text{state} \]

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  \text{operator} must be one of the following:
  - \text{!=}: does not equal
  - \text{==}: equals

- **state**
  Specifies the WSP state for this rule definition.
  \text{state} must be one of the following:
  - \text{close}
  - \text{response-error}
  - \text{response-ok}
  - \text{waiting-for-response}

Usage
Use this command to specify a rule definition to analyze user traffic based on a WSP state.

Example
The following command creates a WSP rule definition for analyzing user traffic using a WSP state of \text{connecting}.

\[ \text{wsp \ state} = \text{connecting} \]
**wsp tid**

This command defines a rule definition to analyze and charge user traffic using WSP Transaction Identifier (TID).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] wsp tid operator tid_value
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **tid_value**
  Specifies the transaction identifier for this rule definition.
  `tid_value` must be an integer from 0 through 255.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WSP tid.

**Example**

The following command creates a rule definition for analyzing user traffic using a WSP TID value of 22:

```plaintext
wsp tid = 22
```
wsp total-length

This command defines a rule definition to analyze and charge user traffic using WSP total packet length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] wsp total-length operator total_length
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!`: does not equal
  - `<`: less than equals
  - `=`: equals
  - `>=`: greater than equals

- **total_length**
  Specifies the total length of the WSP packet including payload for this rule definition.
  `total_length` must be an integer from 1 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the WSP total length.

**Example**
The following command creates a WSP rule definition for analyzing user traffic using an WSP total length of 2000 bytes:

```plaintext
wsp total-length = 2000
```
wsp transfer-encoding

This command defines a rule definition to analyze and charge user traffic using WSP transfer-encoding.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wsp transfer-encoding [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  **operator** must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  `string` must be of 1 through 127 characters in length.

**Usage**
Use this command to specify a rule definition to analyze user traffic based on WSP transfer-encoding.

**Example**
The following command creates a WSP rule definition for analyzing user traffic containing a WSP transfer encoding that contains the number 7:

```
wsp transfer-encoding contains 7
```
wsp uplink

This command defines a rule definition to analyze and charge user traffic using WSP uplink.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] wsp uplink operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
  • !=: does not equal
  • ==: equals

condition
Indicates the uplink (to the Mobile Node direction) status.
condition must be one of the following:
  • FALSE
  • TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the WSP uplink status.

Example
The following command creates a rule definition for analyzing user traffic using a WSP uplink value of TRUE

wsp uplink = TRUE
**wsp url**

This command defines a rule definition to analyze and charge user traffic using WSP URL.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wsp url [ case-sensitive ]operator url
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **url**
  `url` must be an alpha and/or numeric string of 1 through 127 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the WSP URL.

**Example**

The following command creates a rule definition for analyzing user traffic using a WSP URL of `wsp://wiki.tcl.tk`

```
wsp url = wsp://wiki.tcl.tk
```
**wsp user-agent**

This command defines a rule definition to analyze and charge user traffic using WSP user agent.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wsp user-agent [ case sensitive ] operator user_agent
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **user_agent**
  Specifies the WSP user agent for this rule definition.
  `user_agent` must be an alpha and/or numeric string of 1 through 127 characters in length.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the WSP user agent.

**Example**

The following command creates a rule definition for analyzing user traffic containing a WSP user agent of `test`:

```
wsp user-agent contains test
```
wsp x-header

This command defines a rule definition to analyze and charge user traffic based on WSP extension-headers (x-headers).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wsp x-header name [ case-sensitive ] operator string
```

- **no**
  Removes the specified rule definition.

- **name**
  A unique value that you specify to use for the x-header.
  *name* must be an alpha and/or numeric string of 1 through 31 characters in length.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **string**
  Specifies the value of the extension header.
  *string* must be an alpha and/or numeric string of 1 through 127 characters in length.

**Usage**
Use this CLI to configure any x-header field in WSP and parse it. The extension-header mechanism allows additional header fields to be defined without changing the protocol. The extension-header can be any header fields that are not specified in RFC/standard.

Example
The following command creates a rule definition for analyzing user traffic containing WSP extension-header of test_field and value of test_string

```
wsp x-header test_field = test_string
```
wtp

The following commands define rules for analyzing traffic based on Wireless Transaction Protocol (WTP):
wtp any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for WTP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp any-match operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  Specifies the condition for this rule definition.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the WTP any match status.

**Example**

The following command defines an any match rule definition for analyzing WTP user traffic:

```
wtp any-match = TRUE
```
wtp downlink

This command defines a rule definition to analyze and charge user traffic using WTP downlink.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] wtp downlink operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- !=: does not equal
- ==: equals

condition
Indicates the downlink (from the Mobile Node direction) status.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on a WTP downlink condition.

Example
The following command defines a rule definition for analyzing WTP user traffic based on the WTP downlink condition of TRUE:

wtp downlink = TRUE
**wtp gtr**

This command defines a rule definition to analyze and charge user traffic based on the WTP Group Transmission Flag (GTR).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp gtr operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. 
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **condition**
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a WTP GTR condition.

**Example**
The following command defines a rule definition for analyzing WTP user traffic based on the WTP GTR condition of `TRUE`:

```
  wtp gtr = TRUE
```
wtp pdu-length

This command defines a rule definition to analyze and charge user traffic using WTP Protocol Data Unit (PDU) length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
[ no ] wtp pdu-type operator pdu_length
```

*no*
Removes the specified rule definition.

*operator*
Specifies how to logically match the information in the analyzed field.
*operator* must be one of the following:
- `!=`: does not equal
- `==`: equals

*pdu_length*
Specifies the WTP PDU length, in bytes, for this rule definition.
*pdu_length* must be an integer from 1 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on WTP PDU length (header + payload) in bytes.

**Example**

The following command creates a WTP rule definition for analyzing user traffic using an WTP PDU length of 9647 bytes:

```bash
ftp pdu-length = 9647
```
**wtp pdu-type**

This command defines a rule definition to analyze and charge user traffic based on the WTP Protocol data Unit (PDU) type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp pdu-type operator pdu_type
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  - operator must be one of the following:
    - `!=': does not equal
    - `=': equals

- **pdu_type**
  Specifies the WTP PDU type used for this rule definition.
  - pdu_type must be one of the following:
    - `abort`
    - `ack`
    - `invoke`
    - `negative-ack`
    - `result`
    - `segment invoke`
    - `segment result`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WTP PDU type value.

**Example**

The following command creates a WTP rule definition for analyzing user traffic containing a WTP PDU type `result`:

```
wtp pdu-type result
```
**wtp previous-state**

This command defines a rule definition to analyze and charge user traffic using WTP previous state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp previous-state operator previous_state
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **previous_state**
  Specifies the WTP previous state for this rule definition. `previous_state` must be one of the following:
  - `ack-sent`
  - `init`
  - `invoke-sent`
  - `rcvd`
  - `result-rcvd`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a WTP previous state.

**Example**
The following command creates a WTP rule definition for analyzing user traffic using a WTP previous state of `ack_sent`:

```
  wtp previous-state = ack-sent
```
wtp rid

This command defines a rule definition to analyze and charge user traffic based on the WTP Re-transmission Indicator (RID) flag.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] wtp rid operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- ! =: does not equal
- =: equals

condition
condition must be one of the following:

- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on a WTP RID.

Example
The following command creates a rule definition for analyzing user traffic containing a WTP RID condition of TRUE:

wtp rid = TRUE
**wtp state**

This command defines a rule definition to analyze and charge user traffic using WTP state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp state operator state
```

- `no`
  Removes the specified rule definition.

- `operator`
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- `state`
  Specifies the WTP state for this rule definition. `state` must be one of the following:
  - `ack-sent`
  - `close`
  - `init`
  - `invoke-sent`
  - `rcvd`
  - `result-rcvd`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WTP state.

**Example**
The following command creates a WTP rule definition for analyzing user traffic using a WTP state of `close`:

```
wtp state = close
```
**wtp tid**

This command defines a rule definition to analyze and charge user traffic based on the WTP Transaction Identifier (tid).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp tid [ operator ] tid_value
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `=`: equals

- **tid_value**
  Specifies the transaction identifier for this rule definition.
  `tid_value` must be an integer from 0 through 65535.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WTP TID.

**Example**

The following command creates a rule definition for analyzing user traffic containing a WTP TID value of 22:

```
wtp tid = 22
```
wtp transaction class

This command defines a rule definition to analyze and charge user traffic based on the WTP Transaction Class (TCL) state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp transaction class operator transaction_class
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified rule definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>operator</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to logically match the information in the analyzed field. <code>operator</code> must be one of the following:</td>
</tr>
<tr>
<td>• ≠: does not equal</td>
</tr>
<tr>
<td>• =: equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>transaction_class</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the WTP TCL for this rule definition. <code>transaction_class</code> must be an integer from 0 through 2.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to specify a rule definition to analyze user traffic based on a WTP transaction class.

**Example**
The following command creates a WTP rule definition for analyzing user traffic using a WTP transaction class of 2:

```
wtp transaction class = 2
```
**wtp ttr**

This command defines a rule definition to analyze and charge user traffic based on the WTP Trailer Transmission flag (TTR).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp ttr operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **condition**
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WTP TTR condition.

**Example**

The following command defines a rule definition for analyzing WTP user traffic based on the WTP TTR condition of `TRUE`:

```
wtp ttr = TRUE
```
wtp uplink

This command defines a rule definition to analyze and charge user traffic using WTP uplink.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] wtp uplink operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **condition**
  Indicates the uplink (to the Mobile Node direction) status.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**
Use this command to specify a rule definition to analyze user traffic based on the WTP uplink status.

**Example**
The following command creates a rule definition for analyzing user traffic using a WTP uplink value of `TRUE`:

```
wtp uplink = TRUE
```
WWW

The following commands define rules for analyzing traffic based on World Wide Web (WWW):
www any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for WWW.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www any-match operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
- ! =: does not equal
- =: equals

condition
Specifies the condition for this rule definition.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on the WWW any match status.

Example
The following command defines an any match rule definition for analyzing WWW user traffic:

www any-match = TRUE
**www content type**

This command defines a rule definition to analyze and charge user traffic based on the WWW content type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] www content type [ case-sensitive ] operator content_type
```

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:
  - `!=`: does not equal
  - `!contains`: does not contain
  - `!ends-with`: does not end with
  - `!starts-with`: does not start with
  - `=`: equals
  - `contains`: contains
  - `ends-with`: ends with
  - `starts-with`: starts with

- **content_type**
  `content_type` must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

**Usage**

Use this command to specify a rule definition to analyze user traffic based on a WWW content type.

**Example**

The following command creates a SIP rule definition for analyzing user traffic using a WWW content of `test`:

```
www content type = test
```
www downlink

This command defines a rule definition to analyze and charge user traffic based on the WWW downlink conditions.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www downlink operator condition

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• ==: equals

condition
Indicates the downlink (from the Mobile Node direction) status.
condition must be one of the following:
• FALSE
• TRUE

Usage
Use this command to specify a rule definition to analyze user traffic based on a WWW downlink condition.

Example
The following command defines a rule definition for analyzing WWW user traffic based on the WWW downlink condition of TRUE.

www downlink = TRUE
**WWW first-request-packet**

This command defines a rule definition to analyze and charge user traffic based on the Wide Web (WWW) first-request-packet.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] www first-request-packet operator condition
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - `!=`: does not equal
  - `==`: equals

- **condition**
  Specifies the condition for this rule definition.
  *condition* must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to specify a rule definition to analyze user traffic based on the WWW first request packet.

**Example**

The following command creates an WW rule definition for analyzing user traffic testing for the first-request-packet equals *TRUE*:

```plaintext
www first-request-packet = TRUE
```
www header-length

This command defines a rule definition to analyze and charge user traffic based on the WWW packet header length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\[
\text{[ } \text{no } \text{]} \text{ www header-length } \text{operator header_length}
\]

- \text{no}
  - Removes the specified rule definition.

- \text{operator}
  - Specifies how to logically match the information in the analyzed field.
    - \text{! =}: does not equal
    - \text{< =}: less than or equals
    - \text{=} : equals
    - \text{> =}: greater than or equals

- \text{header_length}
  - Specifies the WWW packet header length, in bytes, for this rule definition.
    - \text{header_length} must be an integer from 0 through 65535.

Usage

Use this command to specify a rule definition to analyze user traffic based on a WWW packet header length.

Example

The following command creates an HTTP rule definition for analyzing user traffic using an WWW packet header length of 10000:

\[
\text{www header-length } = 10000
\]
www host

This command defines a rule definition to analyze and charge user traffic based on the WWW host.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www host [ case-sensitive ] operator host_name

- **no**
  Removes the specified rule definition.

- **case-sensitive**
  Default: Disabled.
  This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  *operator* must be one of the following:
  - !=: does not equal
  - !contains: does not contain
  - !ends-with: does not end with
  - !starts-with: does not start with
  - =: equals
  - contains: contains
  - ends-with: ends with
  - starts-with: starts with

- **host_name**
  A unique name that you specify for the WWW host.
  *host_name* must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage

Use this command to specify a rule definition to analyze user traffic based on a WWW host name.

Example

The following command creates a WWW rule definition for analyzing user traffic using a WWW host of *host1*:

```
www host = host1
www payload-length

This command defines a rule definition to analyze and charge user traffic based on the WWW payload length.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www payload-length operator payload_length

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
• !: does not equal
• <=: less than or equals
• =: equals
• >=: greater than or equals

payload_length
Specifies the WWW payload length for this rule definition. payload_length must be an integer from 1 through 4000000000.

Usage
Use this command to specify a rule definition to analyze user traffic based on a WWW payload length.

Example
The following command creates a WWW rule definition for analyzing user traffic using a WWW payload length of 10000:

www payload-length = 10000
**www pdu-length**

This command defines a rule definition to analyze and charge user traffic based on the WWW Protocol Data Unit (PDU) length.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] www pdu-length operator pdu_length
```

---

**no**
Removes the specified rule definition.

---

**operator**
Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:

- `!=`: does not equal
- `<=`: less than or equals
- `==`: equals
- `>=`: greater than or equals

---

**pdu_length**
Specifies the WWW PDU length, in bytes, for this rule definition.

`pdu_length` must be an integer from 0 through 65535.

---

**Usage**
Use this command to specify a rule definition to analyze user traffic based on WWW PDU length (header + payload) in bytes.

---

**Example**
The following command creates an FTP rule definition for analyzing user traffic using a WWW PDU length of 9767 bytes:

```
www pdu-length = 9767
```
www previous-state

This command defines a rule definition to analyze and charge user traffic based on the previous state of WWW.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www previous-state operator previous_state

no
Removes the specified rule definition.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:
  • !=: does not equal
  • ==: equals

previous_state
Specifies the WWW previous state for this rule definition. previous_state must be one of the following:
  • init
  • response-error
  • response-ok
  • waiting-for-response

Usage
Use this command to specify a rule definition to analyze user traffic based on a WWW previous state.

Example
The following command creates a WWW rule definition for analyzing user traffic using a WWW previous state of init:

www previous-state = init
### www reply code

This command defines a rule definition to analyze and charge user traffic based on the WWW reply code arguments.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
(no) www reply code operator response_code
```

- **no**
  Removes the specified rule definition.

- **operator**
  Specifies how to logically match the information in the analyzed field.
  `operator` must be one of the following:
  - `!=`: does not equal
  - `<=`: less than or equals
  - `=`: equals
  - `>=`: greater than or equals

- **response_code**
  A unique value that you specify to use for the response.
  `response` must be an integer from 100 through 599.

**Usage**
Use this command to specify a rule definition to analyze WWW user traffic based on a reply code rule definition.

**Example**
The following command defines a rule definition for analyzing WWW user traffic using a reply code of 110:

```
www reply code = 110
```
www state

This command defines a rule definition to analyze and charge user traffic based on the current state of WWW.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www state operator state

- no
  Removes the specified rule definition.

- operator
  Specifies how to logically match the information in the analyzed field. 
  operator must be one of the following:
  - !=: does not equal
  - ==: equals

- state
  Specifies the WWW state for this rule definition. 
  state must be one of the following:
  - close
  - response-error
  - response-ok
  - waiting-for-response

Usage
Use this command to specify a rule definition to analyze user traffic based on a WWW state.

Example
The following command creates a WWW rule definition for analyzing user traffic using a WWW state of close:

www state = close
www transfer-encoding

This command defines a rule definition to analyze and charge user traffic based on the WWW transfer encoding.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www transfer-encoding [ case-sensitive ] operator string

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: does not equal
• !contains: does not contain
• !ends-with: does not end with
• !starts-with: does not start with
• =: equals
• contains: contains
• ends-with: ends with
• starts-with: starts with

string
A unique name that you specify for WWW transfer encoding.
string must be an alpha and/or numeric string of 1 through 127 characters in length, and can contain punctuation characters.

Usage
Use this command to specify a rule definition to analyze user traffic based on a WWW transfer encoding string.

Example
The following command creates an HTTP rule definition for analyzing user traffic using a WWW transfer encoding string of *user1*:

```
www transfer-encoding = user1
```
www url

This command defines a rule definition to analyze and charge user traffic based on the WWW URL.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] www url [ case-sensitive ] operator url

no
Removes the specified rule definition.

case-sensitive
Default: Disabled.
This keyword makes the rule case sensitive. By default, rule definitions are not case sensitive.

operator
Specifies how to logically match the information in the analyzed field. operator must be one of the following:

- !=: does not equal
- !contains: does not contain
- !ends-with: does not end with
- !starts-with: does not start with
- =: equals
- contains: contains
- ends-with: ends with
- starts-with: starts with

url
url must be an alpha and/or numeric string of 1 through 127 characters in length.

Usage
Use this command to specify a rule definition to analyze user traffic based on the WWW URL.

Example
The following command creates a rule definition for analyzing user traffic using the WWW URL www.abc.com

www url = www.abc.com
Chapter 183
SCCP Network Configuration Mode Commands

The SCCP Network Configuration Mode is used to configure properties for Signaling Connection Control Part (SCCP) services for SS7.

Signaling Connection Control Part (SCCP) is a routing protocol in the SS7 protocol suite in layer 4, which provides end-to-end routing for TCAP messages to their proper database.

```
Exec Mode
  configure
  Global Configuration Mode
    sccp-network
      id_number
    SCCP Network Configuration Mode
```

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

Associates an SS7 routing domain with the SCCP network.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
associate ss7-routing-domain rd_id

no associate

no

Removes the association with the SS7 routing domain from the system configuration.

rd_id

This number identifies an already defined SS7 routing domain.

rd_id: enter an integer from 1 through 12.
```

Usage

Use this command to associate SS7 routing domain configurations with SCCP network configurations.

Example

The following command associates the SCCP network with SS7 routing domain 2:

```
associate ss7-routing-domain 2
```
**description**

This command defines a string that describes the SCCP network. The description is used for operator reference.

**Product**
SGSN, HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
description string
```

```
no description
```

<table>
<thead>
<tr>
<th>string</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is a string to describe the SCCP network.</td>
</tr>
</tbody>
</table>
| *string* must be an alphanumeric string from 1 through 127 characters in length. If there are spaces in the string the string must be enclosed in double-quotes. For example; “This is a Description”.

```
no
```

Removes the description from the system configuration.

**Usage**

Use this command to configure a description of this SCCP service for operator reference.

**Example**

The following command sets the description to “This is the SCCP Service Number 1”:

```
description "This is the SCCP Service Number 1."
```
destination

This command configures the SCCP network destination information. Use this command multiple times to set all of the destination information required.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
destination dpc point_code { name route_name | next-hop | ssn subsys_num | version sccp_ver }
```

```
no destination dpc_code [ name route_name | ssn subsys_num | version sccp_ver ]
```

no
Deletes the specified destination information from the SCCP network configuration.

dpc point_code
Specifies the SCCP destination point code.
point_code: Must be in SS7 point code dotted-decimal ###.###.### format or decimal ####### format.

name route_name
The name of the SCCP destination route.
route_name: enter an alphanumeric string from 1 through 64 characters in length.

next-hop
Associates the next destination defined in the SS7 routing domain.

ssn subsys_num
The destination subsystem number.
subsys_num: enter an integer from 1 through 255.

version sccp_ver
sccp_ver: enter one of the following to select the SCCP variant:
  • ANS188
  • ANS192
  • ANS196
  • BELL05
  • GSM0806
  • ITU88
  • ITU92
**ITU96**

**Usage**
Use this command to configure the destination information for the SCCP network.

**Example**
The following commands set the name of the destination route to default_route, the subsystem number to 1, and the variant version to ITU96, all with a destination point code of 1:

```bash
destination dpc 1 name default_route
destination dpc 1 ssn 1
destination dpc version ITU96
```
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Return to the Exec mode.
exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

---

**Usage**

Return to the global configuration mode.
global-title-translation

This command associates a GTT address-map with this SCCP network.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
global-title-translation address-map instance instance
no global-title-translation address-map instance instance
```

```
no
Deletes the GTT address-map instance associated with this SCCP network.

instance
This value uniquely identifies a specific previously defined instance of a GTT address-map.
instance: enter an integer from 1 to 4096.
```

Usage
Use this command to link a GTT address-map, configured with the GTT Address Map configuration mode, to a specific SCCP network configuration.

Example

```
global-title-translation address-map instance gtt-map1
```
hop-count

This command specifies the hop count for this SCCP network.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

hop-count hop_cnt

default hop-count

default

Resets the hop-count value to the system default of 5.

hop_cnt

The hop count to assign to this SCCP network.

hop_cnt: enter an integer from 1 to 5.

Usage

Use this command to define the hop count for this SCCP network.

Example

The following command sets the hop count to 3:

hop-count 3
self-point-code

This command specifies the SS7 point code for this SCCP service.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

self-point-code point_code

no self-point-code

point_code
Defines the point code to assign to this SCCP network service.

point_code: value entered must adhere to the point code variant selected when the SCCP network instance was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- a string of 1 to 11 combined digits ad period.

Usage
Use this command to assign the self point code to use for this SCCP service.

Example
The following command sets an ITU-based point code for this SCCP service:

    self-pointcode 4.121.5

The following command removes the configured self-point code:

    no self-pointcode
timeout

This command configures the timeout parameters for this SCCP network.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

timeout { attack-timer | congestion-timer | conn-est-timer | crd-timer | decay-timer | iar-timer | ias-timer | interval-timer | reassembly-timer | release-timer | repeat-release-timer | reset-timer | sst-timer } *

default timeout

go timeout timer

attack-timer time
Defines the time before the attack timer expires.
time: enter an integer between 1 and 10.

congestion-timer time
Defines the time before the congestion timer expires.
time: enter an integer between 1 and 10.

conn-est-timer time
Defines the time before the connection timer expires.
time: enter an integer between 6 and 12.

crd-timer time
Defines the time before the coordinated-state-change timer expires.
time: enter an integer between 60 and 120.

decay-timer time
Defines the time before the decay timer expires.
time: enter an integer between 1 and 10.

iar-timer time
Defines the time before the inactivity–receive timer expires.
time: enter an integer between 60 and 120.

ias-timer time
Defines the time before the inactivity–send timer expires.
time: enter an integer between 30 and 60.
timeout

interval-timer time
Defines the time before the interval timer expires.
\textit{time}: enter an integer between 6 and 12

reassembly-timer time
Defines the time before the reassembly-timer expires.
\textit{time}: enter an integer between 10 and 20

release-timer time
Defines the time before the release-assembly timer expires.
\textit{time}: enter an integer between 1 and 2

repeat-release-timer time
Defines the time before repeat-release timer expires.
\textit{time}: enter an integer between 1 and 2

reset-timer time
Defines the amount of time before the reset timer expires.
\textit{time}: enter an integer between 1 and 2

sst-timer time
Defines the amount of time before the subsystem status test timer expires.
\textit{time}: enter an integer between 5 and 1200

default
Resets the timeout parameter to the system default.

no
Deletes the specified timer configuration.

Usage
Use this command to assign timeout timers and timeout values for this SCCP service.

Example

\texttt{timeout reset-timer 75}
Chapter 184
Service Redundancy Protocol Configuration Mode Commands

The Service Redundancy Protocol Mode is used to configure properties for Interchassis Session Recovery services.

![Diagram]

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

server redundancy-protocol

Srvc. Redundancy Protocol Config Mode
```

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

Binds the service to the IP address of the local chassis.

Product
HA, GGSN,

Privilege
Security Administrator, Administrator

Syntax

bind address {IPv4 _address | IPv6_address}

no bind address

no
Removes the IP bind address.

IPv4 _address | IPv6_address
The system IP address.

Usage
Defines the IP address of the local chassis defined as part of the Interchassis Session Recovery configuration.

Example

bind address 1.1.1.1
chassis-mode

Defines the chassis’s operational mode - primary or backup - for Interchassis Session Recovery.

Product
HA, GGSN,

Privilege
Security Administrator, Administrator

Syntax

chassis-mode { primary | backup }

default chassis-mode

  default
  Resets the chassis mode to the default setting of backup.

  primary
  Configures the system as the primary chassis operating in active state.

  backup
  Configures the system as the backup chassis operating in standby state.

Usage
Sets the chassis mode (primary or backup) for the system within the framework of Interchassis Session Recovery.

Example

chassis-mode primary
checkpoint session duration

Configures check pointing for Interchassis Session Recovery.

Product
HA, GGSN,

Privilege
Security Administrator, Administrator

Syntax

checkpoint session duration duration

default checkpoint session duration

default
Resets the checkpoint session duration to the default setting of 60 seconds.

duration
The amount of time (in seconds) that a call must be active before it is check pointed. duration must be an integer from 1 through 65535.

Usage
Sets the amount of time the chassis waits before check pointing an existing call session.

Example

checkpoint session duration 6500
configuration-interval

Defines the configuration validation interval.

**Product**
HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
configuration-interval interval
```

default configuration-interval

---

**default**

Resets the configuration interval to the default setting of 3600 seconds.

---

**interval**

The amount of time (number of seconds) between one configuration validation and the next configuration validation. interval must be an integer from 1 through 65535.

---

**Usage**

This configures the interval between configuration validations of the primary and backup chassis.

---

**Example**

```
configuration-interval 34
```
**dead-interval**

The timeout interval before a peer is determined to be down.

**Product**

HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
dead-interval interval

default dead-interval
```

**default**

Resets the dead interval to the default setting of 30 seconds.

**interval**

The amount of time (in seconds) for the dead interval. interval must be an integer from 1 through 65535.

**Usage**

This command specifies the amount of time that one chassis waits to receive a communication from a peer before the listening chassis determines that the peer chassis is down.

**Example**

```
dead-interval 65
```
delay-interval

Configure the delay time, for starting the dead timer, after configuration files are loaded.

Product
HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
delay-interval interval

default delay-interval
```

```
default
   Sets / Restores default value assigned for specified parameter.

interval
   The amount of time (in seconds) for the delay interval. interval must be an integer from 1 through 65535.
```

Usage
This configures interval for starting the dead timer, after configuration files are loaded.

Example
```
delay interval 65
```
end

Exits the service recovery mode and returns to the Exec mode.

**Product**
HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the Context Configuration mode.

Product
HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the context configuration mode.
hello-interval

Defines the lapse time between sending the hello message.

Product
HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
hello-interval interval
default hello-interval
```

**default**
Resets the hello interval to the default setting of 10 seconds.

**interval**
The lapse time (in seconds) between sending the hello message. interval must be an integer from 1 through 65535.

Usage
This command configures the hello interval - the amount of time that lapses between the sending of each hello message. Each chassis sends the other chassis a hello message at the expiration of every hello interval.

Example

```
hello-interval 35
```
monitor authentication probe

Enables the monitoring of the connection between the primary chassis and a specified RADIUS server.

Product
HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] monitor authentication probe context context_name { IPv4_address | IPv6_address } port port_number
```

- **no**
  Turns off the monitoring.

- **context context_name**
  Identifies the context being used.

- **IPv4 _address | IPv6_address**
  Defines the IP address of the RADIUS server to be monitored.

- **port port_number**
  Identifies a specific port for the authentication probe. port_number must be the port for the AAA server.

Usage
This command initiates monitoring of the connection between the primary chassis and the specified AAA server through the use of authentication probe packets. If the connection drops, the standby chassis becomes active.

Example

```
monitor authentication probe context test1 1.1.1.1 port 1025
```
monitor bgp

Enables monitoring of the connection between the specified BGP peer and the primary chassis.

**Product**
HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] monitor BGP context context_name IPv4_address
```

- **no**
  Disables monitoring.

- **context context_name**
  Identifies the context being used.

- **IPv4_address | IPv6_address**
  Defines the IP address of the BGP peer to be monitored.

**Usage**

This command initiates monitoring of the connection between the primary chassis and the specified BGP peer through the use of authentication probe packets. If the connection drops, the standby chassis becomes active.

**Example**

```
monitor bgp context test 125.2.1.56
```
peer-ip-address

Specifies the IP address for the peer chassis.

**Product**

HA, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
peer-ip-address { IPv4_address | IPv6_address }

no peer-ip-address
```

**Usage**

This command is used to identify the peer chassis in the Interchassis Session Recovery configuration. From the primary’s perspective, the peer is the backup and from the backup’s perspective, the peer is the primary.

**Example**

```plaintext
peer-ip-address 1.1.1.1
```
priority

Sets the initial Interchassis Session Recovery priority of each peer chassis.

**Important:** `priority` takes affect only during simultaneous initializing of all chassis in an Interchassis Session Recovery configuration, and only if a misconfiguration has both chassis in the same mode (both Primary or both Backup).

**Product**
HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
priority priority_value
default priority
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the priority to the default setting of 125.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>priority_value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The priority for the HA. <code>priority_value</code> must be an integer from 1 through 255.</td>
</tr>
</tbody>
</table>

**Usage**

This command determines which chassis transitions to the Active state when all chassis have the same mode configuration. `priority` acts as a tie breaker for the state determination only when all chassis initialize simultaneously. The chassis with the higher priority (higher number) becomes Active while the chassis with the lower priority (lower number) becomes Standby.

Once chassis become operational (after initialization), if there is an event requiring a chassis change of state, then each chassis returns to its previous state (Active or Standby) after both chassis recover.

**Example**

`priority 5`
route-modifier

Sets the route modifier for the peer chassis.

Product
HA, GGSN

Privilege
Security Administrator, Administrator

Syntax

route-modifier threshold threshold_value

default route-modifier

---

default

Resets the route modifier to the default setting of 16.

threshold_value

The value that causes the route-modifier counter to be reset to the initial value. threshold_value must be an integer from 2 through 32.

---

Usage

This command is used to determine when the route modifier should be reset to its initial value to avoid rollover.

---

Example

route-modifier threshold 10
Chapter 185
SGSN APN Policy Configuration Mode Commands

The SGSN APN Policy configuration mode provides the commands to configure the access point name (APN) parameters specific to a particular SGSN operator policy.

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
address-resolution-mode

Identify the address resolution mode for this SGSN APN policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

address-resolution-mode { fallback-for-dns | local }

default address-resolution-mode

default
Resets the configuration to the default value; i.e. fallback-for-dns.

fallback-for-dns
Default: Enabled
This keyword instructs the system to first attempt DNS resolution. If this fails, then the system is to use locally configured addresses, if available.

local
Default: Disabled
This keyword instructs the system not to use DNS query and to only use locally configured addresses.

Usage
Use this command to specify the DNS query or local address resolution for this SGSN APN policy.

Example
The following command sets the address resolution mode to attempt the DNS resolution first and if failed attempt to use available local address:

address-resolution-mode fallback-for-dns
CC

This command provides the configurables to define the charging characteristics for this SGSN APN policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

cc { local-value-for-scdrs behavior bit_value profile index_bit | prefer { hlr-value-for-scdrs | local-value-for-scdrs } }

remove cc { local-value-for-scdrs | prefer }

remove

Removes the charging characteristics configuration for this APN policy.

local-value-for-scdrs behavior bit_value profile index_bit

Defaults: bit_value = 0x0; index_bit = 8

This keyword sets the SGSN APN policy to configure the value of the behavior bits and profile index for the charging characteristics for S-CDRs locally, when the HLR does not provide values for this. If the HLR provides the charging characteristics with behavior bits and profile index and operator want to ignore it, then specify prefer local-value-for-scdrs keyword with this command.

bit_value: Must be a hexadecimal value between 0x0 and 0xFFF.

index_bit: Must be an integer value from 1 to 15.

Some of the index values are predefined according to 3GPP standard:

- 1 for hot billing
- 2 for flat billing
- 4 for prepaid billing
- 8 for normal billing

prefer { hlr-value-for-scdrs | local-value-for-scdrs } 

Default: hlr-value-for-scdrs

Specifies preference for using charging characteristics settings received from HLR or set by SGSN locally.

- hlr-value-for-scdrs: Sets the operator policy to use charging characteristics settings received from HLR for S-CDRs. This is the default preference.

- local-value-for-scdrs: Sets the operator policy to use charging characteristics settings from SGSN only for S-CDRs.

Usage

Use this command to set the APN policy behavior in operator policy to use charging characteristic for S-CDRs either from HLR or locally from SGSN.

The charging characteristics parameters are configurable from SGSN Operator Policy Configuration mode too. For generation of M-CDRs the parameters configured in SGSN Operator Policy Configuration mode will
prevail but for generation of S-CDRs the parameters configured in this SGSN APN Policy Configuration mode will prevail.

**Example**
The following command configures the APN policy not to use charging characteristics setting received from HLR for S-CDR generation.

```
cisco cc prefer hlr-value-for-scdrs
```
**direct-tunnel**

This command defines the permission for direct tunnel establishment by GGSNs resolved by this APN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
direct-tunnel not-permitted-by-ggsn
remove direct-tunnel
```

- **remove**
  Removes the configured policy of not to permit direct tunnel by GGSNs resolved by this APN.

- **not-permitted-by-ggsn**
  Default: Disabled.
  Specifies that a direct tunnel is not permitted by the GGSN resolved by this APN.

**Usage**
Use this command to enable/disable the permission for establishment of direct tunnels between RNC and GGSN.

**Example**
The following command configures the SGSN not to permit the direct tunnel with the GGSN which is resolved by this APN policy:

```
direct-tunnel not-permitted-by-ggsn
```
**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the previous configuration mode.
**gateway-address**

Configures the address of the gateway GPRS support node (GGSN) with priority to activate the GGSN. It also provides the load balancing through weight for specific GGSN address in this APN policy.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gateway-address ip_address { priority priority | weight weight }
no gateway-address ip_address
```

**no**
Removes the preconfigured/defined GGSN address from this APN policy.

**ip_address**
Specifies the IP address for the GGSN in standard IPv4 or IPv6 notation.

**priority priority**
Specify the priority for the configured GGSN address for SGSN address selection. If one GGSN fails to respond, the next priority level GGSN is selected.

`priority` is an integer from 1 to 100 to assign a priority to the GGSN IP address. Note that the lower the integer, the higher the priority so that 1 is the highest priority.

**weight weight**
Specifies the weight (importance) assigned to a GGSN for load balancing.

`weight` is an integer from 1 to 100 to give a weight to the GGSN IP address. If a weight is assigned to an address for that APN, then load balancing (of primary CPC requests) depends on the weight value.

For example:

```
GGSN1 172.16.130.1 weight 30 and GGSN2 172.16.130.3 weight 70
```

With this configuration, 30% of the activation requests for this APN will go to GGSN1 and 70% of the requests will go to GGSN2. Also note, the sum of the weights does not need to be 100. The calculation of weight percentiles is carried out proportionally; so the following configuration will also yield the same 30% - 70% results:

```
GGSN1 172.16.130.1 weight 6 and GGSN2 172.16.130.3 weight 14
```

**Usage**

Use this command to provide a priority and load balancing in GGSN selection through APN policy. Note that keyword priority and weight can not be used simultaneously in one APN policy. A maximum of 16 GGSN address can be configured with this command in an APN policy.
Example

gateway-address 123.123.123.1 priority 2
gtp

This command enables (by adding a configuration statement) or disables (by removing the configuration statement) the GTPC private extension. This command is available in releases 9.0 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```plaintext
gtp private-extension loss-of-radio-coverage send-to-ggsn [ send-to-peer-sgsn ]
remove gtp private-extension loss-of-radio-coverage send-to-ggsn [ send-to-peer-sgsn ]
```

remove

Including this keyword, as part of the command, disables the inclusion of the GTPC private extension, thereby disabling the Overcharging Protection feature.

private-extension

This keyword is required as part of the `gtp` command to instruct the SGSN to set a proprietary GTPC private extension in the LORC Intimation IEs, in the event of loss of radio coverage (LORC). These private extension are only understood by a GGSN with an Overcharging Protection license.

loss-of-radio-coverage send-to-ggsn

This keyword set is required as part of the `gtp` command to instruct the SGSN to forward the private extension ‘flag’ to the GGSN in the event of loss of radio coverage (LORC).

send-to-peer-sgsn

This optional keyword instructs the SGSN to also forward the LORC private extension to the peer SGSN.

Usage

`gtp private-extension` is one of the two commands required to enable the Overcharging Protection feature. The second command sets the RANAP cause code in the Iu Release to enable the SGSN detect the LORC state of the MS/UE. This second command is configured in the IuPS service and is explained in the IuPS Service Configuration Mode chapter.

When there is a loss of coverage and the Overcharging Protection feature is enabled with the `gtp private-extension` command, then the SGSN includes the proprietary private extension in the GTP LORC Intimation IE messages. This LORC IE is also included in UPCQ, DPCQ, and SGSN Context Response GTP messages.

Refer to the SGSN Overview chapter of the SGSN Administration Guide for functional information regarding the Overcharging Protection feature.
Example
Use the following command to have the SGSN send the GGSN the GTPC private extension in the LORC Intimation IE:

```
gtp private-extension loss-of-radio-coverage send-to-ggsn
```
**ip**

Use this command to define the IP parameters for this APN policy.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
ip { qos-dscp { { downlink | uplink } { background | conversational | interactive | streaming } + } | source-violation { deactivate [ all-pdp | exclude-from accounting | linked-pdp | tolerance-limit ] | discard [ exclude-from-accounting ] | ignore }

default ip { qos-dscp [ downlink | uplink ] | source-violation }no qos-dscp { { downlink | uplink } { background | conversational | interactive | streaming } + }
```

---

**Important**: All parameters not specifically configured will be included in the configuration with default values.

**default**

Resets the configuration to the default values.

**qos-dscp**

Configures the diffserv code point marking to be used for sending packets of a particular 3GPP QoS class. Defaults are **downlink** with:

- conversational - ef;
- streaming - af11;
- interactive 1 - ef;
- interactive 2 - af21;
- interactive 3 - af21;
- background - be

**downlink | uplink**

Configures the packets for either downlink or uplink direction. **downlink** and **uplink** configuration must include one or more of the following:

- **background** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP background class. Must be followed by a DSCP marking

- **conversational** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP conversational class. Must be followed by a DSCP marking

- **interactive** - Configures the DSCP marking to be used for packets of sessions subscribed to different traffic priorities in the 3GPP interactive class. Must be followed by a traffic handling priority: 1, 2, or 3.
• **streaming** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP streaming class. Must be followed by a DSCP marking

---

### DSCP marking options

Downlink and uplink configuration options must include a DSCP marking, supported options include:

- **af11** - Designates use of Assured Forwarding 11 PHB
- **af12** - Designates use of Assured Forwarding 12 PHB
- **af13** - Designates use of Assured Forwarding 13 PHB
- **af21** - Designates use of Assured Forwarding 21 PHB
- **af22** - Designates use of Assured Forwarding 22 PHB
- **af23** - Designates use of Assured Forwarding 23 PHB
- **af31** - Designates use of Assured Forwarding 31 PHB
- **af32** - Designates use of Assured Forwarding 32 PHB
- **af33** - Designates use of Assured Forwarding 33 PHB
- **af41** - Designates use of Assured Forwarding 41 PHB
- **af42** - Designates use of Assured Forwarding 42 PHB
- **af43** - Designates use of Assured Forwarding 43 PHB
- **be** - Designates use of Best Effort forwarding PHB
- **ef** - Designates use of Expedited Forwarding PHB

---

### source-violation

Configures settings related to IP source-violation detection with one of the following criteria:

- **deactivate** - Deactivate the PDP context with one of the following conditions:
  - **all-pdp** - Deactivates all PDP context of the MS/UE. Default is to deactivate errant PDP contexts.
  - **exclude-from-accounting** - Excludes packets having an invalid source IP address from the statistics used in the accounting records.
  - **linked-pdp** - Deactivates all associated pdp contexts (primary and secondary). Default is to deactivate errant pdp context.
  - **tolerance-limit** - Configures maximum number of allowed ip source violations before the session is deactivated.
  - **discard** - Discards errant packets, can include the following option:
  - **exclude-from-accounting** - Excludes packets having an invalid source IP address from the statistics used in the accounting records.
  - **ignore** - Ignore checking of packets for MS/UE IP source violation.

---

### Usage

This command is used to configure a range of IP functions to be associated with the APN policy; such as:

- SGSN action to detection of IP source violations,
- DSCP marking for downlink and uplink configuration per traffic class,
- QoS class diffserv code.
Example
Use the following command so the SGSN does not check incoming packets for IP source violation information.

```
ip source-violation ignore
```
pdp-data-inactivity

Configures APN policy regarding PDP data inactivity.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
pdp-data-inactivity { action { deactivate [ all-pdp | linked-pdp ] | detach-when { all-pdp-inactive | any-pdp-inactive } } | timeout minutes minutes }

default pdp-data-inactivity { action | timeout }

no pdp-data-inactivity
```

default
Resets the APN policy configuration to the default values for PDP data-inactivity.

no
Disables the PDP data-inactivity configuration defined for the APN policy.

action
Defines the action to be taken if PDP data-inactivity occurs:
- **deactivate** - defines which PDP context should be deactivated:
  - **all-pdp** - deactivates all PDP contexts.
  - **linked-pdp** - deactivates only linked PDP contexts.
- **detach-when** - defines the condition that warrants a detach:
  - **all-pdp-inactive** - detach when all PDP contexts are inactive.
  - **any-pdp-inactive** - detach when any PDP context is inactive.

timeout minutes minutes

minutes: Must be an integer from 1 to 1440. Note that even though the timeout is set for minutes, the configuration displays in seconds.

Usage
Use this command to define how the SGSN will handle a situation where the PDP is not fully active. Repeat the command, as needed, to configure more than one keyword-controlled function.

Example

---

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01

4889
Use the following command to have the SGSN deactivate all PDP contexts associated with the APN when it detects the PDP is inactive:

```
pdp-data-inactivity action deactivate all-pdp
```

Use the following command to have the SGSN wait 2 minutes after detecting PDP data inactivity:

```
pdp-data-inactivity timeout 2
```
qos class

This command configures Quality of Service (QoS) parameters for traffic class configured for this APN policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

qos class { background | conversational | interactive | streaming } [qualif_option ]

default qos class { background | conversational | interactive | streaming } [qualif_option ]

default
Sets the APN policy to default QoS parameters for the specified traffic class.

class
Defines the class of service for this APN policy. Configuration must include one of the following class options:

• background - selects background class of service and can include one of the qualifying options.
• conversational - selects conversational class of service and can include one of the qualifying options.
• interactive - selects interactive class of service and can include a qualifying option.
• streaming - selects streaming class of service and can include a qualifying option.

qualif_option
Qualifying options include:

• gbr-down - guaranteed bit rate downlink; Enter an integer from the range 1 to 256000 kbps.
• gbr-up - guaranteed bit rate uplink in kbps. Enter an integer from 1 to 256000 kbps.
• mbr-down - maximum bit rate downlink. Enter an integer from the range 1 to 256000 kbps.
• mbr-up - maximum bit rate uplink in kbps. Enter an integer from 1 to 256000 kbps.
• min-transfer-delay - minimum transfer delay in milliseconds. Enter an integer from 80 to 4000.
• residual-bit-error-rate - 
  ● background residual-bit-error-rate range is from 4*10^-4 to 6*10^-8. Enter one of the following integers, where:
    • 4: represents 4*10^-3
    • 7: represents 10^-5
    • 9: represents 6*10^-8
• Conversational residual-bit-error-rate range is from $5 \times 10^{-2}$ to $10^{-6}$. Enter one of the following integers, where:
  • 1: represents $5 \times 10^{-2}$
  • 2: represents $10^{-2}$
  • 3: represents $5 \times 10^{-3}$
  • 5: represents $10^{-3}$
  • 6: represents $10^{-4}$
  • 7: represents $10^{-5}$
  • 8: represents $10^{-6}$

• Interactive residual-bit-error-rate range is from $4 \times 10^{-4}$ to $6 \times 10^{-8}$. Enter one of the following integers, where:
  • 4: represents $4 \times 10^{-3}$
  • 7: represents $10^{-5}$
  • 9: represents $6 \times 10^{-8}$

• Streaming residual-bit-error-rate range is from $5 \times 10^{-2}$ to $10^{-6}$. Enter one of the following integers, where:
  • 1: represents $5 \times 10^{-2}$
  • 2: represents $10^{-2}$
  • 3: represents $5 \times 10^{-3}$
  • 5: represents $10^{-3}$
  • 6: represents $10^{-4}$
  • 7: represents $10^{-5}$
  • 8: represents $10^{-6}$

• sdu - signalling data unit, must include one of the following options:

  • delivery-order: Enter one of the two following options:
    • no: without delivery order
    • yes: with delivery order

  • erroneous: Enter one of the two following options:
    • no: erroneous SDUs will not be delivered
    • no-detect: erroneous SDUs are not detected (‘-‘)
    • yes: erroneous SDUs will be delivered

  • error-ratio: the SDU error-ratio range is from $10^{-3}$ to $10^{-6}$. Enter an integer from 1 to 6, where:
    • 3: represents $10^{-3}$
    • 4: represents $10^{-4}$
    • 6: represents $10^{-6}$
max-size: defines the maximum number of octets (size) of the SDU. Enter an integer from 10 to 1502.

Usage
Use this command to define the qualifying options for each QoS class parameter defined for this APN policy. Repeat the command as often as needed with different keywords to define all required QoS criteria.

Example
Use the following command to define a background QoS class qualified with mbr-down.

```
qos class background mbr-down 5600
```
**qos prefer-as-cap**

This command specifies operational preferences for QoS parameters, specifically QoS bit rates.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
quos prefer-as-cap { both-hlr-and-local | hlr-subscription | local }
remove qos prefer-as-cap
```

**Important:** Command and keyword names have changed. `prefer` has become `prefer-as-cap` and `hlr` has become `hlr-subscription`. These changes will not impact configuration generated with earlier releases as the keywords are aliases for the previous names.

**remove**

Removes previous configuration changes and resets the default.

**both-hlr-and-local**

This keyword instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the HLR subscription.

**hlr-subscription**

Default. Instructs the SGSN to take QoS bit rates from the HLR configuration and use HLR rate as the capping value for session establishment.

**local**

Instructs the SGSN to take QoS bit rate from the local configuration and use it for session establishment.

**Usage**

Use this command to instruct the SGSN to take QoS configuration as the bit rate for session establishment.

**Example**

Following command specifies use of the bit rate in subscription at the HLR:

```
qos prefer-as-cap hlr-subscription hlr
```

Instruct the SGSN to cap the bit rate with the lower rate of the two configurations, HLR or local:
qos prefer-as-cap both-hlr-and-local
qos rate-limit direction

Configure the parameters and actions governing the subscriber traffic flow if it violates or exceeds configured peak or committed data rates.

This command can be entered multiple times to specify different combinations of traffic direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (i.e. it accepts all of the SGSN-provided values for the PDP context).

Additional information on the QoS traffic policing functionality is located in the System Enhanced Feature Configuration Guide.

Important: This command should be used in conjunction with the max-contexts command to limit the maximum possible bandwidth consumption by the APN.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
qos rate-limit direction { downlink | uplink } [ [ burst-size { auto-readjust [ duration seconds ] | bytes } ] [ class { background | conversational | interactive traffic_priority } ] ] | exceed-action { drop | lower-ip-precedence | transmit } ] [ violate-action { drop | lower-ip-precedence | transmit } ] ] +
```

```
remove qos rate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ]
```

```
remove

Disables the QoS data rate limit configuration for the APN policy.
```

Important: If no Qos Profile is configured, the system’s default behavior is to use the information provided by the SGSN.

```
downlink | uplink
```

Apply the limits and actions configured with the other keywords to the selected link:

```
downlink - This is the direction from GGSN to MS. (from Gn to Iu/Gb).
uplink - This is the direction from MS to GGSN (from Iu/Gb to Gn).
```

```
burst-size [ bytes | auto-readjust [ duration seconds ] ]
```

Default: See the table of class default values in the Usage section below.

The peak burst size allowed. System measurements for this value exclude the GTP and outer packet headers.

Supported options include:

- **bytes**: Must be an integer from 1 through 6000000.
**Important:** It is recommended that the minimum value of this parameter be configured to the greater of the following two values: (1) 3 times greater than packet MTU for the subscriber connection, or (2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate. In addition, if the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

- **auto-readjust:** This keyword enables dynamic burst-size calculation, for traffic policing, at the time PDP Activation/Modification is negotiated using QoS maximum bit-rates and guaranteed bit-rates.

- **duration seconds:** Must be an integer from 1 to 30. This keyword sets the number of seconds that the dynamic burst-size calculation will last. This allows the traffic to be throttled at the negotiated rates.

```plaintext
class { background | conversational | interactive traffic_priority | streaming }
```

Apply the specified limits and actions to PDP contexts of the specified UMTS traffic class. The following classes are supported:

- **background:** Specifies the QOS for traffic patterns in which the data transfer is not time-critical (for example email exchange). This traffic pattern should be the lowest QOS.

- **conversational:** Specifies the QOS for traffic patterns in which there is a constant flow of packets in each direction, upstream and downstream. This traffic pattern should be the highest QOS.

- **interactive traffic_priority:** Specifies the QOS for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. This traffic pattern should be a higher QOS than the background pattern, but not as high as that for the streaming pattern. traffic_priority is the 3GPP traffic handling priority and can be an integer 1, 2 or 3.

- **streaming:** Specifies the QOS for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream. This traffic pattern should be a higher QOS than the interactive pattern, but not as high as that for the conversational pattern.

**Important:** If this keyword is omitted, the same values are used for all classes.

```plaintext
exceed-action { drop | lower-ip-precedence | transmit }
```

Default: See the table of class default values in the Usage section below.
The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop:** Drop the packet

- **lower-ip-precedence:** Transmit the packet after lowering the ip-precedence

- **transmit:** Transmit the packet

```plaintext
violate-action { drop | lower-ip-precedence | transmit }
```

Default: See the table of class default values in the Usage section below.
The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop:** Drop the packet

- **lower-ip-precedence:** Transmit the packet after lowering the IP precedence
### transmit

Transmit the packet

+ This symbol indicates that the keywords can be entered multiple times within a single command.

#### Usage

This command configures the APN’s quality of service (QoS) data rate shaping through traffic policing. Configured actions prevent subscriber flow exceeding or violating configured peak or committed data rate limits.

**Important:** If either `exceed action` or `violate action` is set to “lower-ip-precedence”, this command may override the configuration of the `ip qos-dscp` command in the GGSN service configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service `ip qos-dscp` command configuration can override this APN setting for packets from the GGSN to the Internet.

<table>
<thead>
<tr>
<th>Class: Background</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Conversational</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 16000000</td>
<td>Committed Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td>Exceed Action: lower-ip-precedence</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 1</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 2</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 3</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>
SGSN APN Policy Configuration Mode Commands

qos rate-limit direction

<table>
<thead>
<tr>
<th></th>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps)</td>
<td>16000000</td>
<td>8640000</td>
</tr>
<tr>
<td>Committed Data Rate</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes)</td>
<td>65535</td>
<td>65535</td>
</tr>
<tr>
<td>Exceed Action</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Violate Action</td>
<td>drop</td>
<td>drop</td>
</tr>
</tbody>
</table>

Class: Streaming

<table>
<thead>
<tr>
<th></th>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate(in bps)</td>
<td>16000000</td>
<td>8640000</td>
</tr>
<tr>
<td>Committed Data Rate</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Burst Size(in bytes)</td>
<td>65535</td>
<td>65535</td>
</tr>
<tr>
<td>Exceed Action</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Violate Action</td>
<td>drop</td>
<td>drop</td>
</tr>
</tbody>
</table>

Important: If a subscribed traffic class is received, the system changes the class to background and sets the following parameters: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the “Background” class. The received values are used for responses when traffic policing is disabled.

Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak or committed data-rate bps in uplink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos rate-limit direction uplink violate-action shape transmit-when-buffer-full
```
ranap allocation-retention-priority-ie

This command configures the allocation/retention priority (ARP) IE for this APN policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
ranap allocation-retention-priority-ie subscription-priority priority class [ { background | conversational | interactive | streaming } [ not-pre-emptable | priority | queuing-not-allowed | shall-not-trigger-pre-emptable ] ]
```

**Important:** All parameters not specifically configured will be included in the configuration with default values.

```
[ default | remove | no ] ranap allocation-retention-priority-ie [ subscription-priority priority class [ background | conversational | interactive | streaming ] ]
```

default
Resets the configuration to the default values.

no
Disables the specified configuration

remove
Removes the specified configuration.

```
subscription-priority priority
```

This keyword sets the subscription priority. The lowest number means the highest priority.

`priority` must be an integer from 1 to 3.

```
class
```

Configure allocation retention priority for specific QoS traffic classes. Include one or more of the following class options:

- **background** - background class of service
- **conversational** - conversational class of service
- **interactive** - interactive class of service
- **streaming** - streaming class of service

Default values will be included in the configuration for any class configuration not specified.

```
qualifying options
```

For each of the class options, the configuration must include one or more of the following qualifying options:
• **not-pre-emptable**
• **priority** - smallest number is the highest priority. Value must be an integer from 1 to 15
• **queuing-disallowed**
• **shall-not-trigger-pre-emptable**

When entering more than one option, we recommend that you do it in the order in which they are listed.

+ This symbol indicates that the keywords can be entered multiple times within a single command.

---

### Usage

Use this command to configure values for the allocation/retention priority (ARP) IE in the radio access bearer (RAB) assignment request message for RANAP that occurs during RAB setup.

This command can be used multiple times to define multiple priorities, with different combinations of **subscription-priority** and **class**.

If the HLR returns a matching value for the subscribed ARP for the desired traffic class, then the SGSN includes the configured qualifying options for the ARP IE in the RANAP message.

If there is no matching configuration, the SGSN includes the following default values for the traffic class (tc) within the ARP IE:

- **Default values for tc=background:**
  - priority-level = (subscribed-value * 3) + 3
  - pre-emption-capability = may-trigger-pre-emption
  - pre-emption-vulnerability = pre-emptable
  - queuing-allowed = yes

- **Default values for tc=interactive:**
  - priority-level = (subscribed-value * 3) + 3
  - pre-emption-capability = may-trigger-pre-emption
  - pre-emption-vulnerability = pre-emptable
  - queuing-allowed = yes

- **Default values for tc=conversational:**
  - priority-level = (subscribed-value * 3) + 2
  - pre-emption-capability = may-trigger-pre-emption
  - pre-emption-vulnerability = pre-emptable
  - queuing-allowed = yes

- **Default values for tc=streaming:**
  - priority-level = (subscribed-value * 3) + 1
  - pre-emption-capability = may-trigger-pre-emption
  - pre-emption-vulnerability = pre-emptable
  - queuing-allowed = yes
Example
The following series of commands define the highest priority for conversational traffic class with priority level 1-10 (Subscribed priority 0-3), PCI of shall-not-trigger-pre-emption, PVI of not-pre-emptable with queuing-not-allowed:

```
ranap allocation-retention-priority-ie subscription-priority 0 priority class conversational not-pre-emptable priority 1 shall-not-trigger-pre-emptable
ranap allocation-retention-priority-ie subscription-priority 1 priority class conversational not-pre-emptable priority 4 shall-not-trigger-pre-emptable
ranap allocation-retention-priority-ie subscription-priority 2 priority class conversational not-pre-emptable priority 7 shall-not-trigger-pre-emptable
ranap allocation-retention-priority-ie subscription-priority 3 priority class conversational not-pre-emptable priority 10 shall-not-trigger-pre-emptable
```
restrict access-type

This command configures the activation restrictions of PDP context on the basis of the access type and QoS class.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
restrict access-type { { gprs | umts } [ qos-class { background | conversational | interactive | streaming } ] } 
no restrict access-type { gprs | umts } [ qos-class ]
default restrict access-type { gprs | umts }
```

**Usage**
Use this command to configure the restriction rules in an APN policy for activation of PDP context on the basis of the access type. It also provides the facility to restrict type of traffic QoS class.
Example
The following command configures the APN policy to restrict all traffic from a GPRS network service having a QoS class of interactive:

```
restrict access-type grps qos-class interactive
```
Chapter 186
SGSN ASP Configuration Mode Commands

The ASP (application server process) Configuration Mode defines the M3UA end-point parameters for a specific SS7 routing domain instance. The ASP instance is generated originally with the SS7 routing domain configuration mode commands.

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

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec Mode.
end-point

This command defines or deletes the IP address and/or port number to be associated with the local SCTP end-point for this ASP. At least one address needs to be configured before the end-point can be activated.

When using the `bind` keyword, this command also activates the end-point once the address has been defined. Once bound, it cannot be reconfigured until it is unbound with the `no end-point bind` command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end-point { address ip_address context context_id | bind | port port_number }

no end-point { address ip_address context context_id | bind }
```

**address ip_address context context_id:**
Specifies the IP address and the context associated with the address for this end-point.
- `ip_address`: must be defined using the standard IPv4 dotted decimal notation or the colon notation of IPv6.
- `context context_id`: a string of 1 to 79 alphanumeric characters to identify the specific context associated with the end-point address.

**bind**
Activates (binds) the end-point.

**Important:** Only use `bind` after you have configured other parameters.

**port port_number**
Identifies the M3UA’s SCTP port associated with this end-point.
- `port_number`: must be an integer from 1 to 65535. Default is 2905.

**no**
Removes the end-point configuration or deactivates the end-point.

**Caution:** Entering this command will terminate all current subscriber sessions for associated peers.

**Usage**
Use this command to manage the ASP end-point. Once the ASP end-point is bound the end-point configuration can not be changed until it is unbound.

**Example**
Activate the end-point with the following command:
end-point bind

Deactivate or unbind the end-point with the following command:

    no end-point bind

Set the end-point port to default for ASP 1 with the following command:

    default asp instance 1 end-point port
**exit**

Exits the current mode and returns to the previous mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the previous mode.
Chapter 187
SGSN Operator Policy Configuration Mode Commands

The SGSN Operator Policy configuration mode enables the operator to specify a single policy with rules governing the services, facilities, and privileges available to one, multiple, or all subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs. By configuring an operator policy, the operator fine-tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers within a defined IMSI range.

**Important:** To create and use an operator policy, you must first define the IMSI range using the `mcc` command. This does not apply to the default operator policy.

The system supports up to 1000 operator policies, including the single operator policy named `default`. This default operator policy must be configured by the user to define limitations to be applied to any IMSIs that are not covered by any other defined operator policy.

Upon accessing this mode, your prompt should look similar to the following:

```
[local]asn5000(config-sgsn-op-policy-<pol_name>)#
```

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

This command defines the name of the accounting context and optionally associates a GTPP group with this SGSN operator policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

accounting context  ctxt_name [ gtpp group  grp_name ]
remove accounting context

remove
Removes the accounting configuration from this SGSN operator policy configuration.

context  ctxt_name
Use this keyword to identify the accounting context.
ctxt_name: Enter a string of 1 to 79 alphanumeric characters.

gtpp group  grp_name
This keyword set identifies the GTPP group, where the GTPP related parameters have been configured in the GTPP Group configuration mode, to associate with this SGSN operator policy.
grp_name: Enter a string of 1 to 63 alphanumeric characters to identify the GTPP group created with the gtpp group command in the Context configuration mode.

Usage
This command can be used to associate a predefined GTPP server group - including all its associated configuration - with a specific operator policy. The GTPP group would have been defined with the gtpp group command in the Context Configuration Mode chapter of the CLI Reference Guide. If the GTPP group is not specified, then a default GTPP group in the accounting context will be used. If this command is not specified, use the name of the accounting context configured in the SGSN service configuration mode (for 3G) or the GPRS service configuration mode (for 2G), either will automatically use a “default” GTPP group generated in that accounting context. If the accounting context is specified in the GPRS service or SGSN service and in an SGSN operator policy, then priority is given to the accounting context of the operator policy.

Example
For this SGSN operator policy, the following command identifies an accounting context called acctng1 and associates a GTPP server group named roamers with defined charging gateway accounting functionality.
accounting context acctng1 gtpp group roamers
**allocate-ptmsi-signature**

This command enables the allocation of a P-TMSI signature.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
allocate-ptmsi-signature
no allocate-ptmsi-signature
default allocate-ptmsi-signature
```

- **no**
  Disables the allocation of the P-TMSI signature.

- **default**
  Resets the configuration value to the default: allocates the P-TMSI signature.

**Usage**
Enable the allocation of the P-TMSI signature.

**Example**
```
allocate-ptmsi-signature
```
apn

This command creates and associates an SGSN access point name (APN) configuration instance with the SGSN operator policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

apn { network-identifier apn_net_id| operator-identifier apn_op_id} +
no { network-identifier apn_net_id | operator-identifier apn_op_id }

default apn

---

no
Disables the specified APN policy.

---

default
Creates a default SGSN APN policy with default values for all parameters.

---

network-identifier apn_net_id

apn_net_id: Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-), to define the GT-address network identifier. For releases 8.0 the maximum number of characters is 63; for releases 8.1 and higher, the maximum number of characters is 62.

---

operator-identifier apn_op_id

apn_op_id: Enter a string of 1 to 18 alphanumeric characters including dots (.). The entry must be in the following format, where # represents a digit: : MNC###.MCC###.GPRS.

---

Usage
Use this command, to create an SGSN APN policy configuration or to access the SGSN APN configuration mode to update/modify the policy. Either of the two keywords can be used to identify the specific APN policy configuration.

---

Example
For this SGSN operator policy, create an APN configuration for network cust1-net:

    apn network-identifier cust1-net
**apn-restriction**

**Description**  With this command, this SGSN operator policy instructs the system to apply APN restrictions at the SGSN-level.

**Product**  SGSN

**Privilege**  Security Administrator, Administrator

**Syntax**

```plaintext
apn-restriction update-policy deactivate restriction

default apn-restriction
```

- **default**
  - Creates a default APN restriction configuration.

- **restriction**
  - Select one of the two restrictions:
    - `least-restrictive`: applies a lower APN restriction value.
    - `most-restrictive`: applies a higher APN restriction value.

**Usage**

Configures the level of restrictions.

**Example**

Apply the lowest level of APN restrictions.

```plaintext
apn-restriction update-policy deactivate least-restrictive
```
apn-selection-default

This command enables/disables and configures the Default APN feature for use when the normal APN selection process fails. This command is available in releases 8.1 and higher.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

apn-selection-default network-identifier apn_net_id [ require-subscription-apn network-identifier apn_net_id ]

no apn-selection-default

no
Delete the configuration statement and disable the Default APN feature.

network-identifier apn_net_id

The network identifier will be used as the default APN name.
apn_net_id: Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-), to define the GT-address network identifier. For releases 8.0 the maximum number of characters is 63; for releases 8.1 and higher, the maximum number of characters is 62.

require-subscription-apn network-identifier apn_net_id

If defined, this APN name must also be included in the subscription data for the Default APN feature to function.
apn_net_id: Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-), to define the GT-address network identifier. For releases 8.0 the maximum number of characters is 63; for releases 8.1 and higher, the maximum number of characters is 62.

Usage

The default APN will be used in error situations when the SGSN cannot select a valid APN via the normal APN selection process.
Within an operator policy, a default APN can be configured for the SGSN to:
- override a requested APN when the HLR does not have the requested APN in the subscription profile.
- provide a viable APN if APN selection fails because there was no "requested APN" and wildcard subscription was not an option.
In either of these instances, the SGSN can provide the default APN as an alternate behavior to ensure that PDP context activation is successful.
attach

This command defines attach-related configuration for this SGSN operator policy.

**Important:** Before using this command, ensure that the appropriate LAC information has been defined with the `location-area-list` command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] attach allow access-type { gprs | umts } location-area-list list_id
[ no ] attach restrict access-type { gprs | umts } { all | location-area-list instance list_id }
[ no ] attach access-type { gprs | umts } { all | location-area-list list_id } failure-code

default attach { access-type { gprs | umts } { all failure-code | location-area-list instance list_id } }
```

- **no**
  Deletes the specified attach configuration that was previously defined with this command for this operator policy.

- **default**
  Restores the default values for the operator policy for the specified parameter.

- **allow**
  Allow re-enables attaches in the configuration after an `attach restrict` command has been used.

- **restrict**
  Restrict attaches (do not accept calls) of specified `access-type` and from specified location areas (defined using either the `all` or `location-area-list` keywords).

- **access-type**
  Defines the type of access to be allowed or restricted.
  - `gprs`
  - `umts`
  If this keyword is not included, then both access types are allowed by default.
all

Instructs the SGSN to apply the command action to all location areas.

`location-area-list instance list_id`

This keyword identifies a location area list already created with the `location-area-list` command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call. Using this keyword with either the `allow` or `restrict` keywords enables you to configure with more granularity.

`list_id` must be an integer between 1 and 5.

`failure-code`

Specify a GMM failure cause code to identify the reason an attach did not occur. This GMM cause code will be sent in the reject message to the MS.

`fail-code` must be an integer from 2 to 111. Default is 14. Refer to the GMM failure cause codes listed below (information has been taken from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
SGSN Operator Policy Configuration Mode Commands

attach

- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

Usage

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the mcc command, then that specific operator policy is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, then do not use the attach command.

Important: Before using this command, ensure that the appropriate LAC information has been defined with the location-area-list command.

Use this command to define this operator policy’s attach configuration.
Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching.
Attachment restrictions can be based on any one or combination of the options, such as location area code or access type. It is even possible to restrict all attaches.
The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Example

For calls under this operator policy, the following command restricts the attaches of all subscribers using the GPRS access type.

   attach restrict access-type gprs all

Use the next command to reverse the previous attach restrict command:

   attach allow access-type gprs all

Or, change the attach restriction to only restrict attaches of GPRS subscribers from specified LACs included in location area list #2 and include failure-code 45 as the reject cause. This configuration requires two CLI commands:

   attach restrict access-type gprs location-area-list instance 2
   attach access-type gprs location-area-list instance 2 failure-code 45

In the case of a dual-access SGSN, it is possible to also add a second definition to restrict attaches of UMTS subscribers within the LACs included in location area list #3.

   attach restrict access-type UMTS location-area-list instance 3

Change the configuration to allow attaches for GPRS access for all previously restricted LACs - note that GPRS attaches would still be limited.

   no attach restrict access-type gprs all
Restrict (deny) all GPRS attach requests (coming from any location area) and assign a single failure code for the reject messages. This is a two command process:

```plaintext
attach restrict access-type gprs all
attach access-type grps all failure-code 22
```

Remove the restrictions defined above - so that the access type is reset to the default (both types) and the failure code returns to the default value (14).

```plaintext
default attach access-type gprs all failure-code
```
authenticate

Product
This command enables/disables authentication for procedures like attach and service request.

SGSN

Privilege
Security Administrator, Administrator

Syntax
authenticate { activate | all-events | attach [ access-type | attach-type |
frequency | inter-rat ] | detach | rau | service-request }

no authenticate { activate | attach | detach | rau | service-request }

default authenticate { activate | attach | detach | rau | service-request }

no
Disables and removes the defined authentication configuration for this SGSN operator policy.

default
Resets all parameters to default values for the authentication process configured for this SGSN operator policy.

activate
This command enables/disables authentication for activate requests and allows one or more of the following options to the configuration:

• access-type type : Select one of the two options:
  • gprs
  • umts
• first - Enables/disables authentication for first activate.

• frequency frequency - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

  frequency must be an integer from 1 to 16.

• primary - Enables/disables authentication for every primary activate request.

all-events
Specifies that procedures - attaches, service requests, RAUs, detaches, and activations - will be authenticated. This can be fine-tuned by adding either or both of the following parameters:

• access-type type must be one of the two:
  • gprs
SGSN Operator Policy Configuration Mode Commands

authenticate

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01

SGSN Operator Policy Configuration Mode Commands

• umts

• frequency frequency - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

frequency must be an integer from 1 to 16.

attach

This keyword configures the Attach authentication parameters. It enables/disables authentication for an Attach with a local P-TMSI or Attaches with an IMSI will be authenticated to acquire the CK (cipher key) and the IK (integrity key).

• access-type type : Must be one of the following options:
  • gprs
  • umts

• attach-type type : Must be one of the following options:
  • combined : Authenticates combined GPRS/IMSI Attaches.
  • gprs-only : Authenticates GRPS Attaches only.

• frequency frequency - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

frequency must be an integer from 1 to 16.

• inter-rat: Enables authentication for Inter-RAT Attaches.

detach

This keyword enables/disables and configures the access-type authentication for detach.

access-type type : must be one of the two:
  • gprs
  • umts

rau

This keyword enables/disables and configures authentication for routing area updates (RAUs).

• access-type type : Must be one of the two options:
  • gprs
  • umts

• frequency frequency - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

frequency must be an integer from 1 to 16.

• periodicity duration : Defines the length of time (number of minutes) that authentication can be skipped.

duration : Must be an integer from 1 to 10800.
authenticate

• **update-type**: Defines the type of RAU Request. Select one of the following:
  - combined-update {access-type|with inter-rat-local-ptmsi}
  - imsi-combined-update {access-type|with inter-rat-local-ptmsi}
  - periodic {access-type|frequency|periodicity}
  - ra-update {access-type|with inter-rat-local-ptmsi}

`service-request`

This keyword enables/disables authentication for service request.

  • **frequency** `frequency` - Defines 1-in-N selective authentication of subscriber events - where an event is an attach request, RAU, service request, activate-primary-PDP-context request, or detach request. If the frequency is set for 12, then the SGN skips authentication for the first 11 events and authenticates on the 12th event. `frequency` must be an integer from 1 to 16.

  • **periodicity** `duration` - Defines the length of time (number of minutes) that authentication can be skipped.
    - `duration` - Must be an integer from 1 to 10800.

  • **service-type**: Defines the service request type. Options include:
    - data
    - signalling
    - paging response

**Usage**

Use this command with the **frequency** keyword to determine the support for selective execution of the re-authentication and/or P-TMSI reallocation procedure in case of a 3G service request.

**Example**

Configure authentication to occur after every 10th event for GPRS access.

```
authenticate all-events frequency 9 access-type gprs
```

Disable authentication for Inter-RAT Attaches, use:

```
default authenticate attach inter-rat
```

Enable authentication for Inter-RAT RAU of the combined IMSI type:

```
authenticate rau update-type imsi-combined-update with inter-rat-local-ptmsi
```
CC

**Description** This command defines the charging characteristics to be applied for CDR generation through SGSN operator policy.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
cc { behavior-bit no-records bit_value | local-value behavior bit_value profile index_bit | prefer { hlr-value | local-value } }
```

```plaintext
no cc behavior-bit no-records
```

```plaintext
remove cc { behavior-bit no-records | local-value | prefer }
```

**no**
Disables the charging characteristics configuration of behavior bit from this SGSN operator policy.

**remove**
Removes the configured charging characteristics from this operator policy.

**behavior-bit no-records**

`bit_value`

Default: Disabled
Specify that which behavior bit in charging characteristic is used to no accounting records will be generated.
no-records to indicate which behavior bit in charging characteristics, means that no accounting records should be generated.
If we use a charging characteristics with the no-records bit set, then we won’t generate any accounting records, regardless of what may be configured elsewhere. Use “no” to indicate that there is no such bit.

`bit_value` must be an integer value from 1 through 12.

**local-value behavior**

`bit_value profile index_bit`

Default: bit_value = 0x0
index_bit = 8
This keyword sets the SGSN operator policy to configure the value of the behavior bits and profile index for the charging characteristics when the HLR does not provide value for this.
If the HLR provides the charging characteristics with behavior bits and profile index and operator want to ignore it, then specify **prefer local-value** keyword with this command.
`bit_value` must be a hexadecimal value between 0x0 and 0xFFF.
`index_bit` must be an integer value from 1 through 15.
Some of the index values are predefined according to 3GPP standard:

- **1** for hot billing
- **2** for flat billing
- **4** for prepaid billing
prefer

Default: hlr-value

Specifies preference for using charging characteristics settings received from HLR or set by SGSN locally.

- **hlr-value**: Sets the operator policy to use charging characteristics settings received from HLR. This is the default preference.

- **local-value**: Sets the operator policy to use charging characteristics settings from SGSN only. If no charging characteristics received from HLR then local value will be applicable.

Usage

Use this command to set the SGSN operator policy behavior to use charging characteristic either from HLR or locally from SGSN.

These charging characteristics parameters are configurable from SGSN APN Policy Configuration mode too. For generation of M-CDRs the parameters configured in this mode of SGSN Operator Policy Configuration mode will prevail but for generation of S-CDRs the parameters configured in SGSN APN Policy Configuration mode will prevail.

The first four bits of charging characteristics (use keyword profile) is for the charging trigger profile index and is used to select different charging trigger profiles.

The 12 behavior bits (with keyword local-value behavior) can to enable or disable the CDR generation.

Example

The following command configures the SGSN operator policy not to use records for charging characteristics and to set behavior bit to 2:

```
cc behavior-bit no-records 2
```
charging context

**Description** This command has been deprecated in favor of the `accounting-context` command for configuration of charging per SGSN operator policy.
description

Set to a relevant descriptive string.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

description  description

no description

--------------------
description
Enter an alphanumeric string of 1 to 100 alphanumeric characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotes (" ").

--------------------
no
Removes the description configuration from this SGSN operator policy.

Usage
Define information that identifies this particularly SGSN operator policy.

Example

description  "sgsn1 operator policy carrier1"
direct-tunnel

This command allows direct tunneling if the direct tunneling is supported by destination node.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
direct-tunnel attempt-when-permitted
remove direct-tunnel
```

**Usage**
Use this command to enable the direct-tunnel feature at the operator policy level. To ensure that direct tunnel is supported, check the settings of the `direct-tunnel` commands in the SGSN APN policy configuration mode and the Radio Network Controller (release 8.0) or RNC (releases 8.1 or higher) configuration mode. Direct tunneling must be enabled at these two point to allow direct tunneling for the MS/UE.

**Example**
The following command sets the SGSN operator policy to attempt to setup a direct tunnel if permitted at the destination node:

```
direct-tunnel attempt-when-permitted
```
**dns-ggsn**

Define the context to be used to do DNS lookup.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dns-ggsn context ctxt_name

no dns-ggsn context ctxt_name
```

- **no**
  - Removes the dns-ggsn configuration from this SGSN operator policy.

- **ctxt_name**
  - Enter an alphanumeric string of 1 to 64 alphanumeric characters.

**Usage**

Use this command to define the context to be used to do DNS lookup to find the GGSN address.

**Example**

```plaintext
dns-ggsn context sgsn1
```
**dns-sgsn**

Identify the context to be used to do DNS to find the SGSN Address

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] dns-sgsn context ctxt_name
```

- **no**
  Removes the dns-sgsn configuration from this SGSN operator policy.

- **ctxt_name**
  Enter an alphanumeric string of 1 to 64 alphanumeric characters.

**Usage**
Use this command to configure the context ID for the SGSN address that will be used to do the DNS lookup.

**Example**

```
dns-sgsn context sgsn1
```
encryption-algorithm-umts

Defines the order of preference for the encryption algorithm. This feature is specific to a 3G configuration.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

`encryption-algorithm-umts type`

[ default | no ] encryption-algorithm-umts

default
Resets the encryption-algorithm definition with default values.

no
Disables the encryption-algorithm definition.

type
Enter your first choice, first. After entering the first choice, you are prompted to indicate another type as a second priority choice.

- `uea0` - No encryption algorithm
- `uea1` - uea1 Algorithm
- `uea2` - uea2 Algorithm

Usage
Use this command to determine which UMTS encryption algorithm is to be used first.

Example

`encryption-algorithm-umts uea1 then-uea2`
end

Exits the configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end
equivalent-plmn

Configures the definition for an equivalent PLMNID and the preferred radio access technology (RAT). This command can be entered multiple times.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
equivalent-plmn radio_access_technology {2G | 3g | any} plmnid mcc_number mnc_number priority priority
no equivalent-plmn radio_access_technology {2G | 3g | any} plmnid mcc_number mnc_number
```

Enter one of the following options:
- **2G**: 2nd generation
- **3G**: 3rd generation
- **any**: Any RAT

```
plmnid mcc_number mnc_number
```

- **mcc**: Specifies the mobile country code (MCC) portion of the PLMN’s ID. The number can be any integer between 100 and 999.
- **mnc**: Specifies the mobile network code (MNC) portion of the PLMN’s ID. The number can be any integer between 00 and 999.

```
priority priority
```

Select an integer between 1 and 15 with the highest priority assigned to the integer of the lower numeric value.

Usage

Use the priority option to define the preferred equivalent PLMN to be used.

Example

```
equivalent-plmn radio_access_technology any plmnid mcc 121 mnc 767 priority 2
```
exit

Exits the configuration mode and returns to the previous configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit
gmm information-in-messages

This command provides the configuration to include the information in messages for the GPRS mobility management (GMM) parameters.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

gmm information-in-messages access-type { { gprs | umts } [ network-name { full-text name | short-text name } ] [ send-after { attach | rau } ] }  
[ default | no ] gmm { information-in-messages access-type { gprs | umts } }

no
Disables the GMM configuration from this SGSN operator policy.

default
Sets up a GMM configuration with system default values.

access-type

Must select one of the following options:
  • gprs - General Packet Radio Service network
  • umts - Universal Mobile Telecommunications System network

After selecting the access-type, an additional parameter can be configured:
  • network-name: identifies the network name in either short text or full text.
  • send-after: configures the information in message to send after attachment or Routing Area Update (RAU).

network-name { full-text name | short-text name }

This keyword provides the option to add the network name to the message. The network name will in full text or short text. Possible options are:
  • full-text name: Indicate the network name in full text
  • short-text name: Indicate the network name in short text

send-after { attach | rau }

This keyword configures the information in message to send after attachment or RAU message. Possible options are:
  • attach: Information sent after attachment
  • rau: Information sent after routing area update
Usage

Use this command to configure identifying information about the network that will be included in GMM messages.

Example

default gmm information-in-messages access-type gprs
gmm retrieve-equipment-identity

This command configures the International Mobile Equipment Identity (IMEI) or software version (SV) retrieval and validation procedure for SGSN operator policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```bash
gmm retrieve-equipment-identity { imei | imeisv [ unciphered ] [ then-imei ] } [ verify-equipment-identity [ deny-greylisted ] ]

[ no | default ] gmm retrieve-equipment-identity
```

no
Disables the equipment identity retrieval procedure configured for this SGSN operator policy.

default
Sets the default action of equipment identity retrieval (EIR) procedure configuration from this SGSN operator policy:

- **retrieve-equipment-identity**: Default action is disabled - no retrieval of IMEI/IMEI-SV
- **verify-equipment-identity**: Default action is disabled - no verification with Equipment Identity Register (EIR)

**equipment-identity-type**
Default: disabled
Indicates the type of equipment identity to be configured for operator policy. The possible values are:

- **imei**: International Mobile Equipment Identity
- **imeisv**: International Mobile Equipment Identity - Software Version

**imei**
Indicates the equipment identity retrieval type to International Mobile equipment Identity (IMEI). IMEI is a unique 15 digit number consists of TAC (technical approval code), FAC (Final Assembly Code), SNR (Serial Number), and a check digit.

**imeisv** [ unciphered ] [ then-imei ]
Indicates the equipment identity retrieval type to IMEI with software version (SV). IMEI with SV becomes a unique 16 digit number consists of TAC (technical approval code), FAC (Final Assembly Code), SNR (Serial Number), and 2 digit software version number.

- **unciphered**: This optional keyword enables the unciphered retrieval of IMEI-SV. If this option is enabled the retrieval procedure will get IMEISV (if auth is still pending, get as part of Authentication and Ciphering Response otherwise, via explicit Identification Request after Security Mode Complete).
\*\*\* then-imei: \* This optional keyword enables the retrieval of software version number before the IMEI. If this option is enabled, the equipment identity retrieval procedure will get IMEISV on secured link (after Security mode procedure via explicit Gmm Identification Request), and if MS is not having IMEISV (responded with NO Identity), SGSN will try to get IMEI.

If no other keyword is provided, imeisv will get IMEISV on secured link (after Security mode procedure via explicit Gmm Identification Request).

\*\*\* verify-equipment-identity [ deny-greylisted ]

Default: disabled
This keyword enables the equipment identity validation and validates the equipment identity against EIR.
- \*\*\* deny-greylisted: This keyword finetunes the configuration and enables the restriction to the user having mobile equipment with an IMEI in the EIR’s grey list.

**Usage**

Use this command to enable and configure the procedures for mobile equipment identity retrieval and validation from the EIR identified in the MAP Service configuration mode.

**Example**

The following command enables the SGSN to send ‘check IMEI’ messages to the EIR:

```
gmm retrieve-equipment-identity imei verify-equipment-identity
```
gs-service

This command associates the context of a Gs service interface with an SGSN operator policy.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gs-service gs_svc_name context ctx_name
no gs-service svc_name
```

- **no**
  Removes/disassociates the named Gs service from an SGSN operator policy.

- **gs_svc_name**
  Specifies the name of a specific Gs service for which to display information.
  *gs_svc_name* is the name of a configured Gs service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **context ctx_name**
  Specifies the specific context name where Gs service is configured. If this keyword is omitted, the named Gs service must be exist in the same context as the GPRS/SGSN service.
  *ctx_name* is name of the configured context of Gs service. This can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**Usage**

Use this command to associate a specific Gs service interface with this GPRS service instance.

**Important:** A Gs service can be used with multiple SGSN and/or GPRS service.

**Example**

Following command associates a Gs service instance named *stargsl*, which is configured in context named *star_ctx*, with an SGSN operator policy:

```
gs-service stargsl context star_ctx
```
**gtp send**

This command configures which information elements (IE) this operator policy sends in GTP messages. These IEs are required by the GGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtp send { imeisv | ms-timezone | rat | uli }
remove gtp send { imeisv | ms-timezone | rat | uli }
no gtp send
```

---

**remove**
Removes the specified GTP send definition from the system configuration.

**no**
Disables the specified GTP send configuration.

---

**imeisv**
Instructs the SGSN to include the IMEI (international mobile equipment identity (and software version) of the mobile when sending GTP messages of the type “Create PDP Context Request”.

---

**ms-timezone**
Instructs the SGSN to include this IE in GTP messages of the type “Create PDP Request” and “Update PDP Context Request”. This IE specifies the offset between universal time and local time, where the MS currently resides, in steps of 15 minutes. This IE is sent by default.

---

**rat**
The RAT IE specifies which radio access technology (RAT) is being used by the MS (GERAN, UTRAN, or GAN). Including this keyword instructs the SGSN to include this IE when sending GTP messages of the type “Create PDP Request” and “Update PDP Context Request”. This IE is sent by default.

---

**uli**
The ULI IE specifies the CGI (MCC, MNC, etc.) and SAI of the MS where it is registered. Including this keyword instructs the SGSN to include the IE when sending GTP messages of the type “Create PDP Request” and “Update PDP Context Request”. This IE is not sent by default.
Usage

Use this command to define a preferred set of information to include when GTP messages are sent. Repeat this command multiple times to enable or disable multiple options. This instruction will be implemented when the specific operator policy is applied.

Example

Following command series instructs the SGSN to send ULI and RAT in the GTP messages.

```
gtp send ul
gtp send rat
```
gtpu fast-path

This command enables/disables the network processing unit (NPU) Fast Path support for NPU processing of GTP-U packets of user sessions at the NPU.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
[ remove ] gtpu fast-path
```

- **remove**
  Removes the NPU fast path functionality from an operator policy.

**Usage**

Use this command to enable/disable the NPU processed fast-path feature for processing of GTP-U data packets received from GGSN/RNC. This feature enhances the GTP-U packet processing by adding the ability to fully process and forward the packets through the NPU itself.

**Important:** When enabled/disabled, fast-path processing will be applicable only to new subscriber who establishes a PDP context after issuing this command (enabling GTP-U fast path). No existing subscriber session will be affected by this command.

**Example**

Following command enables the NPU fast path processing for all new subscribers’ session established with this operator policy:

```
gtpu fast-path
```
**integrity-algorithm-umts**

This command configures the order of preference for the Integrity Algorithm used for 3G.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
integrity-algorithm-umts type then_type
```

default integrity-algorithm-umts

default

Creates a configuration defining an order of preference based on system defaults.

```
type
```

Enter one or more of the following options in the order of preference:

- **uia1** - uia1 Algorithm
- **uia2** - uia2 Algorithm

**Usage**
Use this command to determine which integrity algorithm is preferred 3G. This command is configured in tandem with the algorithm type for `encryption-algorithm-umts` command.

**Example**

```
default integrity-algorithm-umts
```
location-area-list

Define the location area list to allow or restrict services in the specified location areas identified by location area code (LAC).

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

location-area-list instance instance area-code area_code [ area_code * ]

no location-area-list instance instance [ area-code area_code ]

no
If the area-code keyword is included in the command, then only the specified area code is removed from the identified list. If the area-code keyword is not included with the command then the entire list of LACs is removed from this operator policy.

instance instance
Specifies an identification for the specific location area list.
instance must be an integer between 1 and 5.

area-code area_code *
This keyword defines the location area codes (LACs) to be used by this operator policy as a determining factor in the handling of incoming calls. Multiple LACs can be defined in a single location-area-list.
area_code must be an integer between 1 and 65535.
* If desired, enter multiple LACs separated by a single blank space.

Usage
Use the command multiple times to configure multiple LAC lists or to modify the list.

Example
The following command creates a location area list for a single area code:

location-area-list instance 1 area-code 514

This command creates a second location area list for with multiple area codes - all separated by a single blank space:

location-area-list instance 2 area-code 514 62552 32 1513

The next command corrects an area code mistake (327 not 32) made in the previous configuration:

location-area-list instance 1 area-code 514 62552 327 1513
location-area-list

Cisco ASR 5000 Series Command Line Interface Reference

OL-22948-01
map

Use this command to configure the optional extensions to MAP messages.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ remove ] map message update-gprs-location [ imeisv | private-extension access-type ]

- remove
  IMEI-SV is not included in the GLU request -- this is the default behavior.

- update-gprs-location
  Includes an GLU message. This keyword-set is required.

- imeisv
  Default: disabled
  Specifies the International Mobile equipment Identity-Software Version (IMEI-SV) information to include in GPRS Location Update (GLU) request message. SGSN will include IMEI-SV if available in message.

- private-extension access-type
  Include specific access-type private extension in the message.

Usage
This command configures optional extensions to MAP messages. The HLR should ignore these extensions if not supported by the HLR.

Example

map message update-gprs-location private-extension access-type
map-service

This command identifies a MAP service to associate with the operator policy and the context in which the service is configured.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
map-service context ctxt_name service map_svc_name
no map-service context

no
Disables use of MAP service with this operator policy.

ctxt_name
Enter an alphanumeric string of 1 to 64 alphanumeric characters.

map_svc_name
Enter an alphanumeric string of 1 to 64 alphanumeric characters.

Usage
Use this command to enable or disable MAP service with this operator policy.

Example
no map-service context
max-attached-subscribers

Defines the maximum number of subscribers allowed to attach at one time.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

max-attached-subscribers number

default max-attached-subscribers

default
Creates a configuration based on a system default.

number
Enter an integer from 1 to 4294967295.

Usage
Use this command to limit the number of simultaneous subscriber sessions.

Example

max-attached-subscribers 1231231234
mcc

This command defines a range of IMSI (the international mobile subscriber identity) numbers upon which an operator policy is based. Specifically, this command identifies: the mobile country code (MCC), and the mobile network code (MNC).

Optionally, the command can define, either or both, the mobile subscriber international number (MSIN - the last portion of the IMSI) and the public land mobile network ID (PLMNID).

⚠️ **Important:** This command is mandatory if an operator policy is to be used. However, you do not need to complete this command if you are using the default operator policy.

### Product
SGSN

### Privilege
Security Administrator, Administrator

### Syntax
```
mcc mcc_num mnc mnc_num [ msin first start_num last stop_num | plmnid id ] +
```

- **mcc**
  - Defines the mobile country code (MCC) of an IMSI.
  - **mcc_num**: Enter a 3-digit number from 100 to 999. 000 to 099 are reserved.

- **mnc**
  - Defines the mobile network code (MNC) of an IMSI.
  - **mnc_num**: Enter a 2 or 3-digit number from 00 to 999.

- **msin**
  - MSIN (mobile subscriber international number) portion of the IMSI.
  - **first start_num**: Defines first MSIN prefix number in a range
  - **last stop_num**: Defines the last or final MSIN prefix number in a range.

- **plmnid**
  - PLMN-ID consists of the MCC (mobile country code) plus the MNC (mobile network code) to identify the public land mobile network (PLMN) for a specific operator. This keyword associates a specific PLMN with this specific SGSN operator policy.

+  
  - This symbol indicates that command can be repeated to create repeated definitions.

### Usage
An IMSI = maximum of 15 digits. An IMSI consists of the MCC (3 digits) + the MNC (2 or 3 digits) + the MSIN (the remaining 10 or 9 digits depending on the length of the MNC).
MCC and MNC are the minimum amount of information required to identify a unique operator policy with IMSI filtering. The MCC and MNC combine uniquely to identify the country and the network operator, for example: Cingular Wireless in the United States = mcc 311 mnc 180

To improve the granularity of call handling, an operator policy with additional IMSI filtering parameters can be defined, to include filtering based on the MSIN, by defining a MSIN range - first (or start-of-range) MSIN and last (or end-of-range) MSIN. The range numbers do not include the maximum allowed for the MSIN but should include a sufficient number to enable the operator policy to filter effectively.

For the most efficient IMSI filter, the operator policy should include all of the above parameters and the PLMN ID which defines the current location of the MS -- this parameter is particularly useful for highlighting which calls are roaming.

And if none of the operator policies contain useful filtering information, then the default operator policy will be applied as the information in this command is never defined for the default operator policy.

The following table will illustrate how these filtering parameters determine which operator policy will govern a call:

<table>
<thead>
<tr>
<th>Operator Policy ID</th>
<th>MCC</th>
<th>MNC</th>
<th>MSINfirst</th>
<th>MSINlast</th>
<th>PLMN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpPol-1</td>
<td>123</td>
<td>45</td>
<td>67890</td>
<td>67898</td>
<td></td>
</tr>
<tr>
<td>OpPol-2</td>
<td>123</td>
<td>45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpPol-3</td>
<td>123</td>
<td>45</td>
<td>67890</td>
<td>67898</td>
<td>23232</td>
</tr>
<tr>
<td>OpPol-4</td>
<td>123</td>
<td>45</td>
<td></td>
<td></td>
<td>23232</td>
</tr>
<tr>
<td>OpPol-5</td>
<td>123</td>
<td>45</td>
<td>6789012</td>
<td>6789019</td>
<td></td>
</tr>
<tr>
<td>OpPol-6</td>
<td>123</td>
<td>45</td>
<td>6789012</td>
<td>6789019</td>
<td>23232</td>
</tr>
<tr>
<td>default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The filtering selects which operator policy will be used to determine how a call is handled - the operator policy that best matches the IMSI. So, a call with IMSI 123456789012345 PLMNID 23232 is best matched with OpPol-6.

In most cases, the operator policy with the most information defined will be used as a combination of PLMNID and IMSI provides the best match. But OpPol-6 won’t always be the best match. Using the table above:

OpPol-1 is the best match for IMSI 123456789011111.
OpPol-2 is the best match for IMSI 123456789099999
OpPol-5 is the best match for IMSI 123456789012345 if the PLMNID is 12344

Example
The following defines an operator policy with country code 310, mobile network code of 33, and PLMN ID of 42244.

```
mcc 310 mnc 33 plmnid 42244
```
network-initiated-pdp-activation

This command configures the Operator Policy to support activation of network-initiated PDP contexts and defines any desired activation restrictions.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
network-initiated-pdp-activation { allow | primary | restrict | secondary } +

allow
Allows either or both primary and secondary network-initiated PDP context activation.

primary
Specifies that only network-initiated primary PDP context activation is to be allowed.

restrict
Restricts network-initiated PDP context activation to either primary or secondary PDP contexts.

secondary
Specifies that only network-initiated secondary PDP context activation is to be allowed.
```

Usage

Use this command to define activation restrictions for network-initiated PDP contexts.

Example

```
etwork-initiated-pdp-activation allow
```
nri

This command specifies the network resource identifier (NRI) stored in bit 17 to bit 23 of Packet-temporary mobile subscriber identity (P-TMSI) to be retrieved by SGSN operator policy.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
nri length length [ value value ]
no nri [value ]
```

**no**
Removes the configured NRI value and location in P-TMSI for retrieval by this SGSN operator policy.

**length length**
Specifies the length of bits to be used in the P-TMSI to retrieve NRI information. This starts from bit 23 of the P-TMSI.

*length* must be an integer from 1 to 6.

**value value**
Specifies the value of the NRI to be retrieved from the P-TMSI. This value should not exceed the maximum possible value for the specified length.

*value* must be an integer from 0 to 63.

Usage
Use this command to retrieve the NRI stored in bit 17 to bit 23 of the packet-temporary mobile subscriber identity (P-TMSI).

Example
The following command specifies the length of NRI information to 5 bit and length of the NRI information to 23:

```
nri length 5 value 23
```
pdp-activate access-type

This command configures the PDP context activation option based on operator’s policy for type of access technology.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
pdp-activate access-type { grps | umts } { all | location-area-list instance instance } failure-code failure_code
```

```
default pdp-activate access-type { grps | umts } { all | location-area-list instance instance } failure-code code
```

default
 Resets the configuration to system default values for PDP context activation request.

access-type { grps | umts }
Specifies the access technology type for PDP context activation.
- **grps**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

all
Default: allow
Configures the system to allow to create all PDP context activation request from MS.

location-area-list instance instance
Specifies the location area instance to create PDP context.
`instance` must be an integer from 1 through 5. The value must be an already defined instance of a LAC list created with the `location-area-list` command.

failure-code code
Default: 8
Specifies the failure code for PDP context activation.
`code` must be an integer from 8 through 112.

Usage
Use this command to configure this policy to allow GPRS/UMTS access through PDP context activation request from MS.

Example

```
Following command configures the system to create the PDP context for request from MS for GPRS access type with location area list instance 2 and failure-code 45.

```
pdp-activate access-type gprs location-area-list 2 failure-code 45
```
pdp-activate allow

This command configures the system to allow the PDP context activation based on operator’s policy for type of access technology.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] pdp-activate allow access-type { gprs | umts } location-area-list instance instance

no
Removes the configured permission to create PDP context on request of PDP context activation from MS for an access type.

access-type { gprs | umts }
Specifies the access technology type for PDP context activation.
- gprs: Enables access type as GPRS.
- umts: Enables access type as UMTS.

location-area-list instance instance
Specifies the location area instance to create PDP context.
instance must be an integer from 1 through 5. The value must be an already defined instance of a LAC list created with the location-area-list command.

Usage
Use this command to configure this policy to allow GPRS/UMTS access through PDP context activation request from MS.

Example
Following command configures the system to allow the PDP context activation for GPRS access type with location area list instance 2.

pdp-activate allow access-type gprs location-area-list instance 2
### pdp-activate restrict

This command configures the system to restrict the PDP context activation based on operator’s policy for type of access technology.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] pdp-activate restrict { access-type { gprs | umts } { all | location-area-list instance instance } | secondary-activation }
```

- **no**
  - Removes the configured restriction on PDP context activation through this command.

- **access-type { gprs | umts }**
  - Specifies the access technology type to restrict PDP context activation.
    - *gprs*: Enables access type as GPRS.
    - *umts*: Enables access type as UMTS.

- **all**
  - Default: allow
  - Configures the system to restrict all PDP context activation request from MS.

- **location-area-list instance instance**
  - Specifies the location area instance to restrict PDP context activation.
    - *list_id* must be an integer from 1 through 5. The value must be an already defined instance of a LAC list created with the `location-area-list` command.

- **secondary-activation**
  - Specifies the type of PDP context to restrict for secondary activation. This keyword restricts the system to create the secondary PDP context on receiving the PDP Context Activation Request from the MS.

**Usage**

Use this command to configure this policy to restrict GPRS/UMTS access through PDP context activation request from MS.

**Example**

Following command configures the system to restrict the PDP context activation for request from MS to access GPRS service with location area list instance 2.

```plaintext
pdp-activate restrict access-type gprs location-area-list instance 2
```
pdp-activate restrict
ptmsi-reallocate

Define P-TMSI reallocation for attach or RAU or service requests.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

ptmsi-reallocate { attach | frequency frequency | interval minutes | routing-area-update | service-request } access-type { gprs | umts }

[ no | default ] ptmsi-reallocate { attach | frequency | interval | routing-area-update | service-request } access-type { gprs | umts }

---

access-type
One of the following options must be used to identify the access-type extension.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

---

no
Disables the definition in the configuration.

---

default
Resets the configuration with system defaults.

---

attach
Enables/disables P-TMSI reallocation for attach with local P-TMSI. IMSI or inter-SGSN attach will always be reallocated.

---

frequency frequency
Enter an integer from 1 to 50 to define how many times a particular message can be skipped.

---

interval minutes
Enter an integer between 60 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure.

---

routing-area-update
Enables/disables P-TMSI -reallocation for RAU (routing area update) with local P-TMSI. Inter-SGSN RAU will always be reallocated.

---

service-request
Enables/disables P-TMSI reallocation for service request.
Usage

Use this command to enable the various parameters that will determine the operation of P-TMSI reallocation.

Example

no ptmsi-reallocate attach access-type gprs
rau-inter

Define acceptable procedure for inter-SGSN routing area updates.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

rau-inter { access-type | allow access-type | restrict access-type } { [ all ]
failure-code fail_code | location-area-list instance instance } }

no rau-inter { allow access-type | restrict access-type } { [ all ] failure-code
fail_code | location-area-list instance instance } }

default rau-inter { allow access-type | restrict access-type } { [ all ]
failure-code fail_code | location-area-list instance instance } }

no
Including ‘no’ as part of the command structure disables the values already configured for parameters specified in the command.

default
Resets the configuration of specified parameters to system default values.

allow access-type
Including this keyword-set with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

• gprs - General Packet Radio Service
• umts - Universal Mobile Telecommunications System

restrict access-type
Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

• gprs - General Packet Radio Service
• umts - Universal Mobile Telecommunications System

location-area-list instance instance
list_id must be an integer between 1 and 5. The value must be an already defined instance of a LAC list created with the location-area-list command.

[ all ] failure-code fail-code
Specify a GMM failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.
all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

`fail-code` must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (information has been taken from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

**Usage**

Use this command to configure the restrictions and function of the inter-RAU procedure.

**Example**
default rau-inter allow access-type gprs location-area-list instance 1
rau-intra

Define acceptable procedure for intra-SGSN Routing Area Updates

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

rau-intra { access-type | allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance } }  

no rau-intra { allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance } }  

default rau-intra { allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance } }  

no
Including ‘no’ as part of the command structure disables the values already configured for parameters specified in the command.

default
Resets the configuration of specified parameters to system default values.

allow access-type
Including this keyword-set with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

restrict access-type
Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

location-area-list instance instance
list_id must be an integer between 1 and 5. The value must be an already defined instance of a LAC list created with the location-area-list command.

[ all ] failure-code fail-code
Specify a GMM failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.
all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

\textit{fail-code} must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (information has been taken from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

\begin{itemize}
  \item 2 - IMSI unknown in HLR
  \item 3 - Illegal MS
  \item 6 - Illegal ME
  \item 7 - GPRS services not allowed
  \item 8 - GPRS services and non-GPRS services not allowed
  \item 9 - MSID cannot be derived by the network
  \item 10 - Implicitly detached
  \item 11 - PLMN not allowed
  \item 12 - Location Area not allowed
  \item 13 - Roaming not allowed in this location area
  \item 14 - GPRS services not allowed in this PLMN
  \item 15 - No Suitable Cells In Location Area
  \item 16 - MSC temporarily not reachable
  \item 17 - Network failure
  \item 20 - MAC failure
  \item 21 - Synch failure
  \item 22 - Congestion
  \item 23 - GSM authentication unacceptable
  \item 40 - No PDP context activated
  \item 48 to 63 - retry upon entry into a new cell
  \item 95 - Semantically incorrect message
  \item 96 - Invalid mandatory information
  \item 97 - Message type non-existent or not implemented
  \item 98 - Message type not compatible with state
  \item 99 - Information element non-existent or not implemented
  \item 100 - Conditional IE error
  \item 101 - Message not compatible with the protocol state
  \item 111 - Protocol error, unspecified
\end{itemize}

\textbf{Usage}

Use this command to configure the restrictions and function of the intra-RAU procedure.

\textbf{Example}
default rau-intra allow access-type gprs location-area-list instance 1
re-authenticate

Enable or disable the re-authentication feature. This command is available in releases 8.1 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
re-authenticate [ access-type { gprs | umts } ]
```

**remove re-authenticate**

---

**remove**

Including this keyword with the command disables the feature. The feature is disabled by default.

**access-type**

Defines the type of access to be allowed or restricted.

* **gprs**
* **umts**

If this keyword is not included, then both access types are allowed by default.

---

**Usage**

Use this command to enable or disable the re-authentication feature, which instructs the SGSN to retry authentication with another RAND in situations where failure of the first authentication has occurred. To address the introduction of new SIM cards, for security reasons a systematic "last chance" authentication retry with a fresh Authentication Vector is needed, particularly in cases where there is an SRES mismatch at authentication.

---

**Example**

```
re-authenticate
```
**reuse-authentication-triplets**

Creates an Operator Policy configuration entry to enable or disable the reuse of authentication triplets in the event of a failure.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no | remove ] reuse-authentication-triplets no-limit
```

- **no**
  This keyword disables the SGSN Operator Policy from reusing triplets.

- **remove**
  This keyword causes the reuse configuration to be deleted from the Operator Policy configuration. This is the default behavior. Triplets are reused.

- **no-limit**
  This keyword enables the SGSN Operator Policy to reuse triplets as needed.

**Usage**

Use this command to enable reuse of authentication triplets.

**Example**

```
reuse-authentication-triplets no limit
```
sgsn-address

Use this command to define the SGSN addresses for the static SGSN address table for peer SGSNs.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sgsn-address rac rac-id lac lac_id [ nri nri ] prefer { fallback-for-dns address { ipv4 ip_address | ipv6 ip_address } | local address { ipv4 ip_address | ipv6 ip_address } }
```

```
o sgsn-address { ipv4 ip_address | ipv6 ip_address } rac rac_id lac lac_id
```

---

**no**
Disables the SGSN address configuration for the designated IP address.

---

**rac rac_id**

*rac_id* identifies foreign RAC of the peer SGSN address to be configured in the static peer SGSN address table.

*rac_id* must be an integer from 1 to 255.

---

**lac lac_id**

*lac_id* identifies foreign LAC of the peer SGSN address to be configured in the static peer SGSN address table.

*lac_id* must be an integer from 1 to 65535.

---

**nri nri**

*nri* identifies the network resource identifier stored in PTMSI (bit 17 to bit 23).

*nri* must be an integer from 0 to 63.

---

**prefer**

Indicate the preferred source of the address to be used.

*fallback-for-dns* - instructs the SGSN to do a DNS query to get the address.

*local* - instructs the system to use the local address present in the configuration.

---

**address ip_address**

- *ipv4* - enter a valid address in IPv4 standard notation.
- *ipv6* - enter a valid address in IPv6 standard notation.
sgsn-number

Define the SGSN’s E.164 number to be used for interactions via the MAP protocol.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sgsn-number E164_number
no sgsn-number
```

- **no**
  Disables the use of this configuration definition.

- **E164_number**
  Enter a string of 1 to 16 digits to identify the SGSN’s E.164 identification.
sgtp-service

Identifies the SGTP service configuration to be used for this operator policy.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sgtp-service context  ctxt_name  service  sgtp_service_name

no  sgtp-service context
```

**Example**

```
sgtp-service context  ctxt_name  service  sgtp_service_name
```
sms-mo

This command configures the operator policy dictating how mobile-originated SMS messages are handled.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
[ remove ]sms-mo { { access-type { gprs | umts } { all-location-areas | location-area-list } | allow access-type { gprs | umts } | restrict access-type { gprs | umts } }

remove
Deletes the specified configuration.

access-type type
Access by SMS will be limited to SMS coming from this network type:
  *gprs
  *umts

allow
Allow either GPRS or UMTS type access for SMS.

restrict
Restrict either GPRS or UMTS type access for SMS.

location-area-list instance instance
instance must be an integer between 1 and 5. The value must identify an already defined LAC list created with the location-area-list command.

failure-code code
code: Must be an integer from 2 to 111.
```

Usage
Configure filtering for SMS-MO messaging.

Example

```
sms-mo access-type gprs all-location-areas failure-code code
```
**sms-mt**

This command configures the operator policy dictating how mobile-terminated SMS messages are handled.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ remove ]sms-mt { { access-type { gprs | umts } { all-location-areas | location-area-list } | allow access-type { gprs | umts } | restrict access-type { gprs | umts } }
```

- **remove**
  Deletes the specified configuration.

- **access-type type**
  Access by SMS will be limited to SMS coming from this network type:
  - *gprs
  - *umts

- **allow**
  Allow either GPRS or UMTS type access for SMS.

- **restrict**
  Restrict either GPRS or UMTS type access for SMS.

- **location-area-list instance instance**
  *instance* must be an integer between 1 and 5. The value must identify an already defined LAC list created with the `location-area-list` command.

- **failure-code code**
  *code*: Must be an integer from 2 to 111.

**Usage**
Configure filtering for SMS-MT messaging.

**Example**

```
sms-mt access-type gprs all-location-areas failure-code code
```
srns-inter

Inter-SRNS (Serving Radio Network Subsystem) relocation.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

\[ \text{srns-inter} \ ( \text{all failure-code} \ | \ \text{allow location-area-list instance instance} \ | \ \text{location-area-list instance instance failure-code code} \ | \ \text{restrict location-area-list instance instance} \) \]

\[ \text{no srns-inter} \ ( \text{allow location-area-list instance instance} \ | \ \text{restrict location-area-list instance instance} \) \]

\[ \text{default srns-inter} \ ( \text{all} \ | \ \text{location-area-list-instance instance instance} \) \]

\[ \text{no} \]
Deletes the inter-SRNS relocation configuration.

\[ \text{default} \]
Resets the configuration to default values.

\[ \text{all failure-code code} \]
Define the failure code that will apply to all inter-SRNS relocations.
\[ \text{code} \]: Must be an integer from 2 to 111.

\[ \text{allow location-area-list instance instance} \]
Identify the location area list Id (LAC Id) that will allow services in the defined location area.

\[ \text{location-area-list instance instance} \]
\[ \text{instance} \]: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the \text{location-area-list} command.

\[ \text{restrict location-area-list instance instance} \]
Identify the location area list Id (LAC Id) that indicates the location areas where services will be restricted.

Usage
This command defines the operational parameters for inter-SRNS relocation.

Example
Use the following command to allow services in areas listed in LAC list #3:
\[ \text{srns-inter allow location-area-list instance 3} \]
srns-intra

Intra-SRNS (Serving Radio Network Subsystem) relocation.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

srns-intra { all failure-code | allow location-area-list instance instance | location-area-list instance instance failure-code code | restrict location-area-list instance instance }

no srns-intra { allowlocation-area-list instance instance | restrictlocation-area-list instance instance }

default srns-intra { all | location-area-list-instance instance }

no

Deletes the intra-SRNS relocation configuration.

default

Resets the configuration to default values.

---

**all failure-code code**
Define the failure code that will apply to all intra-SRNS relocations.

*code*: Must be an integer from 2 to 111.

**allow location-area-list instance instance**
Identify the location area list Id (LAC Id) that will allow services in the defined location area.

**location-area-list instance instance**

*instance*: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the `location-area-list` command.

**restrict location-area-list instance instance**
Identify the location area list Id (LAC Id) that indicates the location areas where services will be restricted.

Usage

This command defines the operational parameters for intra-SRNS relocation.

Example

Use the following command to restrict service in areas listed in the LAC list 1:

```
srns-intra restrict location-area-list instance 1
```
subscriber-control-inactivity

This command defines the time for the subscriber-control inactivity timer. The system seeks to detect inactivity where no PDP context is activated and then starts the timer.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

subscriber-control-inactivity timeout minutes time

( no | default ) subscriber-control-inactivity

no
Deletes the timer configuration.

default
Resets the timer configuration to the default value of 7 days (10080 minutes).

time
This timer is measured in minutes.
time: Enter an integer from 1 to 20160 (two weeks).

Usage
Use this command to configure the timeout timer. After this timer times out the subscriber is detached from the SGSN.

Example

subscriber-control-inactivity timeout minutes 360
**super-charger**

This command enables/disables the SGSN to work with a super-charged network.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
super-charger

remove super-charger
```

**Usage**

By enabling the super charger functionality for 2G or 3G connections controlled by an operator policy, the SGSN changes the hand-off and location update procedures to reduce signalling traffic management.

**Example**

Enable the feature with the following command:

```plaintext
super-charger
```
wildcard-apn

Define the APN to be used in case a wildcard APN is included in the subscriber record.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
wildcard-apn pdp-type pdp-type apn-network-identifier apn_net_id
no wildcard-apn pdp-type pdp-type
```

- **no**
  - Removes the wildcard-apn definition from the configuration.

- **pdp-type pdp-type**
  - `pdp-type` can be one of the following options:
    - `ipv4` - for an ipv4 context
    - `ipv6` - for an ipv6 context
    - `ppp` - for a PPP context

- **apn-network-identifier apn_net_id**
  - `apn_net_id`: Must be one of the APN network Ids defined with the `apn` command in this SGSN operator policy configuration mode.
  - `apn_net_id`: Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-), to define the network identifier. For releases 8.0 the maximum number of characters is 63; for releases 8.1 and higher, the maximum number of characters is 62.

**Usage**

This command is used to define a wildcard APN with the type of PDP context and the APN’s network ID. This wildcard APN would be used when an APN is not identified.

**Example**

Use this command to create an APN wildcard:

```plaintext
wildcard-apn -pdp-type ipv4 apn-network-identifier homern1
```
zone-code

Create a zone code and define one or more LAC Ids to specify service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

zone-code zc_id lac lac_id

[ no ]

no
Removes either a specific LAC Id from the zone-code definition or if lac_id is not included in the command then the entire zone-code definition is removed from configuration.

zc_id
Must be an integer from 1 to 65535.

lac_id
This keyword identifies a location area-code list previously defined with the location-area-list command of this SGSN operator policy configuration mode.
lac_id must be an integer from 1 to 65535.

Usage
Repeat this command to include multiple LAC Ids in the service definition.

Example

zone-code 1 lac 4132zone-code 1 lac 1234zone-code 1 lac 64321
Chapter 188
SGSN Pool Area Configuration Mode Commands

The Pool Area configuration mode configures the parameters used to setup the VLRs to use with a pool area in a Gs service.

```
Exec Mode

configure

Global Configuration Mode

context name

Context Configuration Mode

gs-service name

Gs Service Configuration Mode

pool-area name

Pool Area Configuration Mode
```

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

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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Return to the Exec mode.
exit

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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Return to the previous configuration mode.
hash-value

This command configures the load distribution for the VLRs that service this pool area.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
hash-value { hash_value | range start_value to end_value | non-configured-values
} use-vlr vlr_name

no hash-value { hash_value | range start_value to end_value | non-configured-values }
```

**no**
Removes the configured Gs procedures from this Gs service.

**hash_value**
Specifies the specific hash value for VLR(s).
```
hash_value must be an integer value from 0 through 999.
```

**range start_value to end_value**
Specifies the range of hash values for a VLR.
```
start_value specifies the start value for range of hash and is an integer value from 0 through 999.
start_value must be lower than end_value.
end_value specifies the end value for range of hash and is an integer value from 0 through 999.
end_value must be higher than start_value.
```

**non-configured-values**
This keyword assign all non-configured hash values to use the named VLR.

**use-vlr vlr_name**
Specifies the name of the VLR to be associated with this pool area.
```
vlr_name is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.
```

**Usage**
Use this command to command configures the load distribution for the VLRs that service this pool area as defined in TS 23.236.
The algorithm for selection of VLR from a pool area is based on the hash value computed on the IMSI digits. The SGSN derives a hash value (V) using procedure as defined in TS 23.236. Every hash value from the range 0 to 999 corresponds to a single MSC/VLR node. Typically many hash values may point to the same MSC/VLR node.
This command can be entered multiple times for different hash value.
Example
Following command configure the all non configured hash values to use VLR named \texttt{starvlrl} in this pool area:

\texttt{hash-value non-configured-values use-vlr starvlrl}
lac

This command defines a set of location area code (LAC) values for a pool area.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
lac lac_id +
no lac lac_id
```

More than one `lac_id`, separated by a space, can be entered within a single command.

```
no
Removes the configured LAC value from this pool area configuration.
```

```
lac lac_id
```

Specifies the subscribers’ location area code (LAC) to be associated with this pool area and a specific VLR. This LAC is obtained from the radio area indicator (RAI).

`lac_id`: Must be an integer from 1 through 65535.

```
+  
```

More than one `lac_id`, separated by a space, can be entered within a single command.

**Usage**

Use this command to specify a set of LACs to use for a pool area.

This command can be entered multiple times, subject to a limit of 32 LAC definitions (total for non-pool-area and pool-area configuration) per Gs service.

**Important:** LAC values across multiple pool areas and non-pool-areas must be unique within the Gs service.

**Example**

The following command configures LACs 101, 301, and 222 for the pool area.

```
lac 101 301 222
```
Chapter 189
SGSN PSP Configuration Mode Commands

The Peer-Server Process (PSP) configuration mode provides the commands to create, configure, bind, and manage a specific PSP instance for a SS7 Routing Domain.

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

Defines an association between the PSP instance and an application server process (ASP) instance.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
associate asp instance asp_num
```

```
no associate
```

```
no
```

Removes the association between the PSP and the ASP from the routing domain configuration.

**Important:** Using this command will probably result in the termination of all current subscriber sessions active through the peer-server.

```
asp_num
```

Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.

*asp_num* must be an integer from 1 through 4.

**Usage**
Create an association between a specific peer-server process (PSP) and a specific application server process (ASP) instance. The M3UA end-point of the ASP must be configured prior to configuring the PSP-ASP association. Use the commands defined in the ASP Configuration Mode chapter of the Command Line Interface Reference.

**Example**

```
associate asp instance 2
```
**end**

Exits the configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Change the mode back to the Exec mode.
end-point

This command defines or deletes the IP address to be associated with the local SCTP end-point for the application server process (ASP).

Product  
SGSN

Privilege  
Security Administrator, Administrator

Syntax

```plaintext
end-point [ address ip_address | port port_number ]
no end-point [ address ip_address ]
```

- **port port_number**
  - Identifies the M3UA’s SCTP port associated with this end-point.
  - `port_number`: must be an integer from 1 to 65535.
  - Removes the end-point configuration.

- **no**
  - Removes the ASP end-point association from the PSP configuration.

**Important**: This command can not be used as long as the PSP and the ASP are associated.

Usage

Use this command to manage the ASP end-point. At least one address needs to be configured for the ASP before the end-point can be associated with the PSP.

Example

Set the end-point to IP address 192.168.1.1 with the following command:

```plaintext
end-point address 192.168.1.1
```
exchange-mode

Configures the exchange-mode for the peer-server process.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
exchange-mode [ double-ended | single-ended ]
```

**Usage**
Use this command to toggle the exchange modes for the peer-server process. The default (initial configuration) mode is double-ended.

**Example**

```bash
exchange-mode double-ended
```
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the Global configuration mode.
**psp-mode**

Configures the peer-server process (PSP) operational mode as either client or server mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
psp-mode { client | server }
```

- **client**
The PSP operates as a client.

- **server**
The PSP operates as a server.

**Usage**
Instruct the peer-server process to operate in either client or server mode.

**Example**

```
psp-mode server
```
**routing-context**

Configures the behavior of the routing context in M3UA messages.

---

**Important:** This keyword function is only available in releases 8.1 and higher.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
routing-context { discard-inbound | process-inbound { insert-outbound | suppress-outbound }

default routing-context
```

---

**default**

Include this keyword with the command, to reset the configuration to the system default for routing-context which is a combination of process-inbound and insert-outbound.

---

**discard-inbound**

Sets the routing context received in M3UA messages to be discarded.

---

**process-inbound**

Sets the routing context received in M3UA messages to be processed.

---

**insert-outbound**

Sets the routing context so that it is added in the M3UA messages.

---

**suppress-outbound**

Sets the routing context so that it is suppressed in the M3UA messages.

---

**Usage**

In PSP (singled-ended) configuration mode, the settings for both the local routing context (the SGSN's routing context) and the peer routing context (the RNC's routing context) should be the same. If the routing contexts created at the SGSN and on the peer are different then this can cause the M3UA link to fail. Routing context is an optional parameter when an M3UA association has only one associated peer-server.

---

**Example**

```
 routing-context discard-inbound insert-outbound
```
sctp-alpha

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines a retransmission timeout value.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

sctp-alpha value

default sctp-alpha

value
Defines a percentage (%) that represents the RTO portion of the RTT calculation. This percentage value must be an integer between 0 and 65535.

default
Resets the sctp-alpha to the default value of 5%.

Usage
sctp-alpha is used in conjunction with other commands, such as the sctp-beta command, to determine the round-trip time (RTT) calculations. The Alpha parameter is used to manage load balancing within the SS7 environment for multi-homed peers.

Example

sctp-alpha 256
**sctp-beta**

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines a retransmission timeout value.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-beta value
```

```
default sctp-beta
```

value

Defines a percentage (%) that represents the RTO portion of the RTT calculation. This percentage value must be an integer between 0 and 65535.

```
default
```

Resets the `sctp-beta` to the default value of 10%.

**Usage**

Use this command in conjunction with other commands, such as the `sctp-alpha` command, to determine the round-trip time (RTT) calculations. The Beta parameter is used to manage load balancing within the SS7 environment for multi-homed peers.

**Example**

```
sctp-beta 512
```
sctp-checksum-type

This command selects the type of checksum algorithm to be used.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sctp-checksum-type { adler32 | crc32 }
default sctp-checksum-type
```

---

**adler32**
Selects the Adler-32 type of algorithm as a faster checksum function.

---

**crc32**
Selects the CRC-32, a slower but more reliable 32-bit cyclic redundancy check.

---

**default**
Resets the `sctp-checksum-type` to the default of CRC-32.

---

**Usage**
Use this command to set which type of checksum algorithm the SGSN is to use to validate SCTP packets.

**Example**

```
sctp-checksum-type crc32
```
**sctp-cookie-life**

This command sets the valid life for the SCTP cookie.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
sctp-cookie-life value
```

**default sctp-cookie-life**

```
value
Sets the cookie life value in increments of 100 milliseconds. The range is 50 to 1200.
```

```
default
Resets the sctp-cookie-life value to the default, 600 (= 60 seconds).
```

**Usage**

Use this command to set the SCTP cookie life.

**Example**

```
sctp-cookie-life 60
```
**sctp-max-assoc-retx**

This command sets the maximum number of datagram retransmissions to be associated with this peer server configuration.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-max-assoc-retx value
```

```
default sctp-max-assoc-retx
```

- **value**
  Defines the maximum number of datagram retransmissions for an association. The value must be an integer between 0 and 255.

- **default**
  Resets the default for `sctp-max-assoc-retx` to 10.

**Usage**

Use this command to configure the maximum number of datagram retransmissions for an association. The endpoint will be declared unreachable after `sctp-max-assoc-retx` number of consecutive retransmissions to an endpoint on any transport address.

**Example**

```
sctp-max-assoc-retx 3
```
**sctp-max-init-retx**

This command sets the maximum number of retries to send the INIT datagram.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
sctp-max-init-retx value

default sctp-max-init-retx

value
Sets the maximum number of retries. This value must be an integer between 0 and 255.

default
Resets the default for `sctp-max-init-retx` to 5.
```

**Usage**

Use this command to set the maximum number retries the SCTP layer should make to send the INIT datagram to the peer to open an association.

**Example**

```plaintext
sctp-max-init-retx 3
```
**sctp-max-mtu size**

This command sets the number of bytes that comprise the maximum MTU size.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-max-mtu-size value

default sctp-max-mtu-size
```

- **value**
  Sets the maximum number of bytes for the SCTP MTU size. This value must be an integer between 508 and 65535.

- **default**
  Resets the default for `sctp-max-mtu-size` to 1500.

**Usage**
Use this command to configure the size of the MTU.

**Example**

```
sctp-max-mtu-size 1024
```
**sctp-max-out-strms**

This command sets the maximum number of outgoing streams through the PSP going towards the peer server.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-max-out-strms max#_out_streams
default sctp-max-out-strms
```

**default**

Resets the SGSN’s `sctp-max-out-strms` value to the default of 16.

**max#_out_streams**

The value must be an integer between 1 and 65535. The value should match the peer node’s (STP/SG/RNC/HLR) number of in-bound streams.

**Usage**

Use this command to balance the stream throughput from the PSP to the peer server. The value for this command is used to validate the incoming packets in the SCTP layer.

**Example**

```
sctp-max-out-strms 3500
```
sctp-max-path-retx

This command sets the maximum number of datagram retransmissions for this path.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sctp-max-path-retx value
```

```
default sctp-max-path-retx
```

```
value
Sets the maximum number of datagram retransmission to a destination transport address. This value must be an integer from 0 to 255.
```

```
default
Resets the sctp-max-path-retx default to 5.
```

Usage
Use this command to set the maximum number of datagram retransmissions to a destination transport address. The destination transport address will be declared unreachable after the SGSN exhausts the sctp-max-path-retx number of consecutive retransmissions to a destination transport address.

Example

```
sctp-max-path-retx 10
```
**sctp-rto-initial**

This command sets the initial retransmission timeout for the SCTP.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-rto-initial value

default sctp-rto-initial
```

- **value**
  Sets the timeout in increments of 100 milliseconds. The value must be an integer between 10 and 1200.

- **default**
  Resets the system to the sctp-rto-initial default of 30 (3 seconds).

**Usage**
Use this command to define the initial retransmission timer.

**Example**
```
sctp-rto-initial 240
```
sctp-rto-max

This command sets the maximum retransmission timeout value for the SCTP.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-rto-max value

default sctp-rto-max
```

```
default
Resets the system to the sctp-rto-max default of 600 (60 seconds).
```

```
value
Set the maximum retransmission timeout value in increments of 100 milliseconds and the value must be an integer between 5 and 1200.
```

**Usage**

Use this command to configure the maximum time for retransmissions.

**Example**

The following sets the timeout for 45 seconds:

```
sctp-rto-max 450
```
**sctp-rto-min**

This command sets the minimum retransmission timeout (RTO) value for the SCTP.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-rto-min value
```

```
default sctp-rto-min
```

**default**

Resets the *sctp-rto-min* to the default of 10 (1 second).

**value**

Sets the minimum retransmission timeout in increments of 100 milliseconds. The value must be an integer from 1 to 50.

**Usage**

Use this command to set the minimum time for retransmission before timeout.

**Example**

The following sets the timeout for 2 seconds:

```
sctp-rto-min 20
```
**sctp-sack-frequency**

This command sets the frequency of transmission of SCTP selective acknowledgements (SACK).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-sack-frequency value
```

```
default sack-frequency
```

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the maximum number of datagrams to be received prior to sending a SACK to the peer. The value must be an integer between 1 and 5.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the <code>sctp-sack-frequency</code> default value of 2.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the maximum number of datagrams to be received before a SACK must be sent to the peer. The `sctp-sack-frequency` is used in conjunction with the `sctp-sack-period` to control the generation of SACK, depending on which one occurs first.

**Example**

```
sctp-sack-frequency 3
```
**sctp-sack-period**

This command sets the delay before sending an SCTP selective acknowledgement (SACK).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sctp-sack-period value
```

```
default sack-period
```

---

**value**

Sets the maximum time, in increments of 100 milliseconds, before the system must send a SACK to the peer. The value must be an integer from 0 to 5.

---

**default**

Resets the system to the `sctp-sack-period` default value, 2 (=200 milliseconds).

---

**Usage**

Use this command to set the time the SCTP waits to send a SACK.

**Example**

```
sctp-sack-period 120
```
sctp-suppress-alarm

This command enables/disables the suppression of alarms for SCTP path failure between two peer endpoints.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ]sctp-suppress-alarm path-failure self-end-point-address
orig_ipv4_address peer-end-point-address peer_ipv4_address

no
Disables the pre-configured alarm suppression for SCTP path failure.

path-failure
This keyword specifies that the alarm suppression is for SCTP path failure between two peer nodes.

self-end-point-address orig_ipv4_address
This keyword specifies the IP address of the originating endpoint.
orig_ipv4_address is the IP address of originating endpoint in IPv4 dotted decimal notation.

peer-end-point-address peer_ipv4_address
This keyword specifies the IP address of the peer endpoint.
peer_ipv4_address is the IP address of peer endpoint in IPv4 dotted decimal notation.

Usage
Use this command to configure the path failure alarm suppression. This command ignores the alarms generated on SCTP path failure.

Example
The following command suppresses the path failure alarms occurred in SCTP path between originating peer address 1.2.3.4 and peer endpoint 6.7.8.9:

sctp-suppress-alarm path-failure self-end-point-address 1.2.3.4 peer-end-point-address 6.7.8.9
timeout

This command sets the times for various timeout timers.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
timeout { m3ua-periodic-dest-audit dest_timeout | sctp-bundle bundle_time | sctp-heart-beat hrt_bt_timeout }

default timeout sctp-heart-beat
```

default
Resets the system to the default values.

```
m3ua-periodic-dest-audit dest_timeout
```
Sets the period (in increments of seconds) between the DAUD messages while auditing a destination state.

*dest_timeout*: Must be an integer from 1 to 65535. Default is 2.

```
sctp-bundle
```
Sets the SCTP bundle timeout value in increments of 100 milliseconds, with a range of 1 to 65535. By default, SCTP bundling is disabled.

```
sctp-heart-beat hrt_bt_timeout
```
Sets the number of seconds in the SCTP heart-beat timer

*hrt_bt_timeout*: This value is an integer between 1 and 300. Default is 30.

Usage
Use this command to configure timers. Repeat the command with each of the keywords to set values for each.

Example

```
timeout m3ua-periodic-dest-audit 120
```
Chapter 190
SGSN Service Configuration Mode Commands

The SGSN Service configuration mode is used within the global configuration mode to specify the 3G operations of the SGSN and the available SGSN services for a specific context.

SGSN Service works with MAP Service, SGTP Service, GTPP Group, and IuPS Service. All five of these services must be configured to enable a 3G SGSN to communicate with other elements within a UMTS network.

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

This command defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
accounting { cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } } + | context cntx_name }
```

default accounting cdr-types

no accounting { cdr-types | context }

---

default

Returns the system to default settings for the selected type of CDR.

---

no

Removes the pre-configured type of CDR generation for accounting from the SGSN service.

---

```
cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } } +
```

Default: enabled

Defines the types of CDRs to be generated within the specified SGSN service for accounting:

- **mcdr**: Enables generation of M-CDRs.
- **scdr**: Enables generation of S-CDRs.
- **sms**: Enables generation of SMS-type CDRs based on one of the following:
  - **mo-cdr**: SMS CDRs originates from the mobile.
  - **mt-cdr**: SMS CDRs terminates at the mobile.

---

```
+ 
```

Specifies that the specified keywords with in the group can be entered multiple times with a single command.

---

```
context cntx_name
```

Specifies an accounting context to be associated with the SGSN service.

*cntx_name*: Define a string of 1 to 79 alphanumeric characters.

---

Usage

Use this command to define the type of CDRs to generate for SGSN service. By default all type of CDRs are generated. Note that change of this configuration will be applied to new call and/or to new PDP contexts only.
By default, generation of the S-CDR, M-CDR, SMS-MT-CDR, and SMS MO-CDR types is enabled.

Example
The following command configures the system to generate CDRs of M-CDR type for accounting in the current SGSN service:

```
accounting cdr-types mcdr
```
cc profile

Configures the charging characteristic (CC) profile with the triggers for generating various types of CDR as defined with the accounting command.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

cc profile profile_bits [ buckets number | interval time | tariff time1 mins hours [ time2 mins hours ] [ time3 mins hours ] [ time4 mins hours ] | volume { downlink down_vol uplink up_vol | total total_vol } ] +

[ no | default ] cc profile profile_bits [ buckets | interval | tariff | volume ]

no
Removes a previously configured CC profile.

default
Returns the specified CC profile to the original default system settings.

profile_bits
Defines the value of the profile bits for the SGSN service.
index can be configured to any integer value from 0 to 15. Some of the values have been predefined according to 3GPP standard:

1 for hot billing
2 for flat billing
4 for prepaid billing
8 for normal billing

buckets number
Specifies the number of statistics container changes in the CDR due to QoS changes or tariff times that can occur before an accounting record (CDR) is closed
Default: 4
number: Must be integer from 1 to 4.

interval time
Specifies the normal time duration (in seconds) that must elapse before closing an accounting record (CDR) provided that any or all of the following conditions occur:
time: Enter any integer from 60 to 4000000.
```
tariff time1 mins hours [ time2 mins hours time3 mins hours time4 mins hours ]
```

Specifies the time-of-day (based on a 24-hour clock) to close the current statistics container in the CDR, but not necessarily the CDR itself. One tariff time must be defined and up to four tariff times can be specified.

**Important:** The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

- **mins:** The minutes of the hour. Enter an integer from 0 to 59.
- **hours:** The hour of the day. Enter an integer from 0 to 23.

```
volume { downlink down_vol uplink up_vol | total total_vol }
```

Specifies the downlink, uplink, and total volumes octet counts that must be met for the closure of the CDR.

- **down_vol:** Enter any integer from 100000 to 1345294336.
- **up_vol:** Enter any integer from 100000 to 40000000.
- **total_vol:** Enter any integer from 100000 to 40000000.

**Usage**

Charging characteristics consist of a profile index and behavior settings. This command configures the profile index for the SGSN’s charging characteristics. The SGSN supports up to 16 profile indexes.

**Example**

The following command configures a profile index of 10 with tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10 tariff time1 07 time2 30 19 time3 07 time4 30 19
```
check-imei-timeout-action

This command configures the action to be taken if a Check-IMEI fails due to a timeout. This command is available in releases 8.1 and higher.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

check-imei-timeout-action [ continue | reject ]

default check-imei-timeout-action

default
Rejects the Attach or ISRAU procedure if a Check-IMEI timeout occurs.

continue
Instructs the SGSN to continue the Attach or ISRAU procedure if a Check-IMEI timeout occurs because the EIR is not reachable. This functionality matches standard call flow.

reject
Instructs the SGSN to reject the Attach or ISRAU procedure if a Check-IMEI timeout occurs.

Usage
Use this command only if the Gf interface (EIR) is available in the network. This command controls the SGSN reaction if the Check-IMEI procedure fails due to a timeout.

The continue option allows the SGSN to go forward with the MS Attach or RAU, if the first Check-IMEI fails to reach the EIR due to a timeout. Any subsequent activity (such as a RAU or Service Request would force another Check-IMEI towards the EIR. If this subsequent MAP Check-IMEI should fail, then the same policy of continuing the procedure would apply.

Example

check-imei-timeout-action continue
core-network

This command specifies the numeric ID for a core network to identify which CN is to be used by the SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

core-network id cn_id

no core-network id

no
Removes the currently configured core network ID from the current SGSN configuration.

id cn_id
This number identifies the core network to connect the SGSN service.

cn_id: Must be an integer from 0 through 65535.

Usage
Use this command to set a global ID to identify this SGSN in the core network.

Example
The following command sets the core network ID for the current SGSN service to 127:

core-network id 127
disable/enable super-charger

This command has been deprecated and replaced by the `super-charger` command. For the commands to configure the SuperCharger feature are explained the *SGSN Operator Policy Configuration Mode* chapter.

**Product**

SSGN
**dns israu-mcc-mnc-encoding**

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query which is sent during the ISRAU.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dns israu-mcc-mnc-encoding { decimal | hexadecimal }
default dns israu-mcc-mnc-encoding
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>decimal</td>
<td>Default. Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.</td>
</tr>
<tr>
<td>hexadecimal</td>
<td>Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query sent during the inter-SGSN RAU (ISRAU). The choice must match the format of the DNS server. For example:

In decimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc310.mcc722.gprs
```

In hexadecimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc0136.mcc02d2.gprs
```

**Example**

Use hexadecimal values for the MCC/MNC in the DNS query.

```
dns israu-mcc-mnc-encoding hexadecimal
```
end

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

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
```end```

Usage
Return to the Exec mode.
exit

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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the context configuration mode.
gmm

This command defines the GPRS mobility management parameters for the SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gmm { T3302-timeout t3302_dur | T3312-timeout t3312_dur | T3313-timeout initial t3313_init [ decrease t3313_decrement | increase t3313_increment ] | T3322-timeout t3322_dur | T3350-timeout t3350_dur | T3360-timeout t3360_dur | T3370-timeout t3370_dur | implicit-detach-timeout impli_detach_dur | max-auth-retransmission auth_retrans | max-identity-retransmission id_retrans | max-page-retransmission page_retrans | max-ptmsi-reloc-retransmission ptmsi_reloc_retrans | mobile-reachable-timeout ms_reach_dur | perform-identity-on-auth-failure | purge-timeout purge_dur | trau-timeout trau_dur }


no gmm { implicit-detach-timeout | max-auth-retransmission | max-identity-retransmission | perform-identity-on-auth-failure }
```

default
Sets the default value for the specified parameter.

T3302-timeout t3302_dur
Default: 10
Specifies the retransmission timer value to guard the GPRS attach or RAU procedure on MS side. t3302_dur is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

T3312-timeout t3312_dur
Default: 54
Specifies the retransmission timer value to guard the RAU procedure initiation on network side. t3312_dur is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

T3313-timeout initial t3313_init [ decrease t3313_decrement | increase t3313_increment ]
Default: 5
Specifies the retransmission timer value to guard the for paging request procedure initiation on network side.
initial \texttt{t3313\_init} is the initial waiting duration in seconds before retransmitting the specific message. \texttt{t3313\_init} must be an integer from 1 through 60.

decrease \texttt{t3313\_decrement}. specifies the decrement of the initial timer value in seconds. \texttt{t3313\_decrement} must be an integer from 1 through 5.

increase \texttt{t3313\_increment}. specifies the increment of the initial timer value in seconds. \texttt{t3313\_decrement} must be an integer from 1 through 5.

\begin{verbatim}
T3322-timeout t3322_dur
Default: 6
Specifies the retransmission timer value to guard the GPRS detach request procedure on network side. \texttt{t3322dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.
\end{verbatim}

\begin{verbatim}
T3350-timeout t3350_dur
Default: 6
Specifies the retransmission timer value to guard the GPRS attach accept/RAU accept/realloc request procedure sent with P-TMSI and/or TMSI on network side. \texttt{t3350dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.
\end{verbatim}

\begin{verbatim}
T3360-timeout t3360_dur
Default: 6
Specifies the retransmission timer value to guard the authentication and cipher request procedure on network side. \texttt{t3360dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.
\end{verbatim}

\begin{verbatim}
T3370-timeout t3370_dur
Default: 6
Specifies the retransmission timer value to guard the identity request procedure on network side. \texttt{t3370dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.
\end{verbatim}

\begin{verbatim}
implicit_detach_timeout impli_detach_dur
Default: 3600
Specifies the retransmission timer value to guard the implicit detach procedure on network side. \texttt{impli\_detach\_dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 3600.
\end{verbatim}

\begin{verbatim}
max-auth-retransmission auth_retrans
Default: 4
Specifies the maximum retransmission of authentication requests allowed. \texttt{auth_retrans} is the number of retries before declaring the authentication failure and must be an integer from 1 through 10.
\end{verbatim}

\begin{verbatim}
max-identity-retransmission id_retrans
Default: 4
Specifies the maximum retransmission of identity requests allowed.
\end{verbatim}
**id_retrans** is the number of retries before declaring the identity failure and must be an integer from 1 through 10.

**max-page-retransmission page_retrans**
Default: 5
Specifies the maximum retransmission of page requests allowed.
**id_retrans** is the number of retries before declaring the paging request failure and must be an integer from 1 through 5.

**max-ptmsi-reloc-retransmission ptmsi_reloc_retrans**
Default: 5
Specifies the maximum retransmission for P-TMSI relocation procedure allowed.
**id_retrans** is the number of retries before declaring the P-TMSI relocation procedure failure and must be an integer from 1 through 5.

**mobile-reachable-timeout ms_reach_dur**
Default: 58
Specifies the retransmission timer value to guard the mobile reachability procedure on network side.
**impli_detach_dur** is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 1440.

**perform-identity-on-auth-failure**
Default: Enabled
Configures the SGSN service to perform an identity check to ascertain the IMSI after an authentication failure on a PTMSI-based message.

**purge-timeout purge_dur**
Default: 10080 (7 days)
Specifies the timer value to guard the detach of MM context procedure on network side.
**impli_detach_dur** is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 20160.
Define the purge timer to hold detached mm-contexts. Default is 10080 mins (7 days).

**trau-timeout trau_dur**
This timer is available in releases 9.0 and higher.
Default: 30
Specifies the number of seconds the “old” 3G SGSN waits to purge the MS’s data. This timer is started by the “old” SGSN after completion of the inter-SGSN RAU.
**trau_dur**: Must be an integer from 5 to 60.

**Usage**
Repeat this command as needed to configure multiple parameters for GPRS mobility management in a UMTS network. This command provides the configuration of timers for mobility procedures and retries for different messages. GMM layer is defined in the 3GPP TS 24.008 (Release 7).

**Example**
Following command configures the timer to wait for 5 mins before retransmitting the message for GPRS attach or RAU procedure on MS side with maximum number of retries as 6 for authentication:

```
gmm T3302-timeout 5 max-auth-retransmission 6
```
gs-service

This command associates a previously defined Gs service interface to MSC/VLR along with its associated context with an SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

`gs-service gs_svc_name context ctx_name`

`no gs-service gs_svc_name`

- `gs_svc_name`
  Specifies the name of a specific Gs service for which to display information. `svc_name` is the name of a configured Gs service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- `context ctx_name`
  Specifies the specific context name where Gs service is configured. If this keyword is omitted, the named Gs service must be exist in the same context as the SGSN service. `ctx_name` is name of the configured context of Gs service. This can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Usage

Use this command to associate a specific Gs service interface with this SGSN service instance.

**Important**: A single Gs service can be used with multiple SGSN and/or GPRS service.

Example

Following command associates a Gs service instance named `stargsl`, which is configured in context named `star_ctx`, with an SGSN service:

```
gs-service stargsl context star_ctx
```
lac

This command defines the location area code (LAC in hexadecimal format.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

    lac  hex

    no  lac

    no
    Erases the lac configuration statement.

    hex
    Enter a hexadecimal number between 0x0 and 0xFFFF
max-pdp-contexts

Configures the maximum number of PDP contexts for a MS (mobile station) that will be supported on this SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

max-pdp-contexts per-ms number

default max-pdp-contexts per-ms

default
Resets the maximum number of PDP contexts per mobile station to the default of 11 for the Gs service configuration

per-ms number
Default: 11
Defines the combined total number of primary and secondary PDP contexts for the SGSN service. number can be an integer from 2 to 11.

Usage
The following example defines 5 as the maximum number of primary and secondary PDP contexts that this SGSN will support for any connected MS.

Example

max-pdp-contexts per-ms 5
mobile-application-part

This command identifies an already defined MAP service (Mobile Application Part service) to associate with the SGSN service. Although the MAP service does not need to be defined in the same context as the SGSN service, there is a one-to-one relationship between a MAP service and an SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

mobile-application-part service map_svc [ context ctx_name ]

no mobile-application-part service

no
Remove the MAP service association from the SGSN service configuration.

service map_svc
Specifies the name of the MAP service to be associated with this SGSN service.
map_svc must be the name of a MAP service previously configured on the system.

context ctx_name
Specifies the name of the context where the MAP service is configured. If the MAP service is not configured in the current context, then the context where it is configured must be specified to enable the SGSN to reach the MAP service.
If this keyword is not specified, the current context is used.
ctx_name: Must be the name of the context where the specified MAP service is configured.

Usage

Use this command to identify the MAP service configuration to be used by the SGSN service configuration. Also use this command to specify the context in which the MAP service configuration was created.
If the MAP service is not identified or if the correct context is not identified, then the SGSN service will not START.

Example

The following command specifies a MAP service named map1 that is configured in the same context as the current SGSN service:

mobile-application-part service map1
network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

network-sharing cs-ps-coordination

default network-sharing cs-ps-coordination

no network-sharing cs-ps-coordination

default
Including this keyword resets the SGSN service to allow the check to be performed.

no
Disables this feature for the SGSN service.

Usage
Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.

3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

Example
Use the following syntax to disable the CS-PS coordination check:

no network-sharing cs-ps-coordination
nri length

This command defines the Network Resource Identifier (NRI) of the SGSN that is stored in the P-TMSI (bits 23 to 18).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nri length  nri_length  {  nri-value  nri_value  |  null-nri-value  null_nri_value  
non-broadcast  mcc  mcc  mnc  mnc  lac  lac_id  rac  rac_id  [  nri-value  nri_value  ]  
no  nri
```

- **no**
  Removes the configured NRI value and location in P-TMSI for retrieval by this SGSN operator policy.
  
  **nri length  nri_length**
  Specifies the number of bits to be used in the P-TMSI, bits 23 to 18, to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.
  
  **nri_length**: Must be an integer from 1 to 6 to identify the number of bits.

- **null-nri-value  null_nri_value**
  This keyword is only available in releases 8.1 and higher. Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the `sgsn offloading` command, see the Exec Mode chapter).
  
  **null_nri_value**: 0 (zero) indicates the keyword is not to be used and 1 to 63 are used to identify the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.

- **non-broadcast  mcc  mcc  mnc  mnc  lac  lac_id  rac  rac_id**
  This keyword set is only available in releases 8.1 and higher.
  
  Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure. Including the MCC and MNC to specify the PLMN because the Iu-Flex feature supports multiple IuPS Services.
  
  **mcc**: identifies the mobile country code, the first part of the PLMN ID. Must be an integer between 100 and 999.
  
  **mnc**: identifies the mobile network code portion of the PLMN ID. Must be a 2- or 3-digit integer between 01 and 999.
  
  **lac_id**: defines a location area code associated with an RNC. Must be an integer between 1 and 65535.
  
  **rac_id**: defines the remote area code to be associated with an RNC. Must be an integer between 1 and 255.
nri-value nri_value

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.

nri_value must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.

Multiple NRI values can be identified by providing multiple nri-values separated by a blank space for example: nri length 6 nri-value 29 43 61

Usage

Use this command to identify the SGSN identified with the NRI in the MS generated P-TMSI. This command adds or removes the Iu Flex configuration for this SGSN service. When using Iu Flex, all keywords must be defined. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.

Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.

When using MOCN mode for network sharing without SGSN pooling, the NRI length and the NRI value should both be used.

Example

The following command specifies the the NRI length as 5 bits, identifies SGSN 23 with LAC 222 and RAC 12 for offloading procedure with NRIs 6 and 41:

```
nri length 5 null-nri-value 34 non-broadcast lac 222 rac 12 nri-value 6
```

**override-lac-li**

This command defines the override location area code (LAC) needed for the function of the lawful intercept feature.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
override-lac-li hex

no override-lac-li
```

- **no**
  Erases the override location area code for this GGSN service from the configuration.

- **hex**
  Enter a hexadecimal number between 0x0 and 0xFFFF
override-rac-li

This command defines the override routing area code needed for the lawful intercept function.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

override-rac-li hex

no override-rac-li

no
Erases the override routing area code for this GGSN service from the configuration.

hex
Enter a hexadecimal number between 0x0 and 0xFFFF
**rac**

This command defines the override routing area code needed for the lawful intercept function.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
rac hex
no rac
```

---

**no**
Erases the routing area code configuration statement.

---

**hex**
Enter a hexadecimal number between 0x0 and 0xFFFF
**ran-protocol**

This command specifies the IuPS service for the SGSN service to use for communication with the RAN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ran-protocol iups-service iups_svc [ context ctx_name ]
```

```
no ran-protocol iups-service
```

- **no**
  
  Removes the IuPS service information from the SGSN service configuration.

- **iups-service iups_svc**
  
  Specifies the name of an IuPS service already configured on the system.
  
  `iups_svc`: Enter an alphanumeric string of 1 to 63 characters.

- **ctx_name**
  
  `ctx_name`: Enter the name of the IuPS context, an alphanumeric string of 1 to 63 characters.

**Usage**

Use this command to configure the IuPS service context that the current SGSN service will use to communicate with the RAN. Up to 8 definitions can be defined for a single SGSN service to allow for multiple PLMNs support.

**Example**

The following command configures the SGSN service to use an IuPS service named `iups1` that has been configured in the same context as the SGSN service:

```
ran-protocol iups-service iups1
```
sgsn-number

This command defines the E.164 number that identifies this particular SGSN service context.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sgsn-number  E.164_number

no sgsn-number
```

```
no
Removes the SGSN number configuration from the SGSN service configuration.

E.164_number
Enter a maximum of 15 digits to define this ‘phone’ number associated with this SGSN service context.
```

Usage
To delete the sgsn-number associated with this SGSN service context, enter:

Example

```
no sgsn-number
```
sgtp-service

This command creates an instance of an SGTP service.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
sgtp-service sgtp_srvc_name
no sgtp-service
```

Usage

```
sgtp_srvc_name
Enter the name of an SGTP service that will be used by this SGSN service
sgtp_srvc_name: Enter a string of 1 to 63 alphanumeric characters.
```

Example

```
sgtp-service sgtp1
```
**sm**

This command configures session management parameters for this SGSN service. This command can be repeated multiple times to configure each parameter individually.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sm { T3385-timeout time | T3386-timeout time | T3395-timeout time | max-actv-retransmission number | max-deactv-retransmission number | max-modf-retransmission number | rab-ass-timeout time | session-inactivity | rns-ctxt-rsp-timeout }
```

```
default sm timer
```

**default**

Resets the selected timer to the system default value.

**T3385-timeout**

Retransmission timer for network-initiated Activate Request. Default is 8 sec

**T3386-timeout**

Retransmission timer for network-initiated Modify Request. Default is 8 sec

**T3395-timeout**

Retransmission timer for network-initiated Deactivate Request. Default is 8 sec

**max-actv-retransmission**

Configures maximum retries for activate PDP ctxt request. Default is 4

**max-deactv-retransmission**

Configures maximum retries for deactivate PDP ctxt request. Default is 4

**max-modf-retransmission**

Configures maximum retries for modify PDP ctxt request. Default is 4

**Usage**

Repeat the command to configure multiple session management parameters for the SGSN service.

**Example**
sm T3385-timeout 5
Chapter 191
SGTP Service Configuration Mode Commands

The SGSN GPRS Tunneling Protocol (SGTP) Service configuration mode provides the configuration of GTP-C and GTP-U related parameters for the SGSN.

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

Exits the configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the Global configuration mode.
gtpc

Configure the GPRS Tunneling Protocol Control (GTP-C) settings for the SGTP service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
gtpc { bind address ip_address | dns-sgsn context ctxt_name | echo-interval seconds | guard-interval seconds | ignore response-port-validation | max-retransmissions num | retransmission-timeout seconds | send { common flags | rab-context } }

no gtpc { bind address ip_address | dns-sgsn context ctxt_name | echo-interval seconds | send { common flags | rab-context } }

default gtpc { echo-interval | guard-interval | ignore response-port-validation | max-retransmissions | retransmission-timeout | send { common flags | rab-context } }
```

---

**no**

Disables the configured GTPC setting.

---

**default**

Resets the specified parameter to its default value.

---

**bind address ip_address**

Binds SGTP service to the IP address of the interface. Enter a standard dotted-quad IPv4 address. The bind address for the `gtpc` and `gtpu` commands should be the same.

---

**dns-sgsn context ctxt_name**

Enter a string of 1 to 79 alphanumeric characters to identify the context name.

---

**echo-interval seconds**

Default: 60

*seconds* must be an integer from 0 through 3600. Configures the duration between echos.

---

**guard-interval seconds**

Default: 100

Configures the interval (in seconds) for which the SGTP maintains responses sent to SGSN. This optimizes the handling of retransmitted messages. This value should be configured to be greater than the SGSN's configuration for max-retries multiple by retry-interval.

*seconds*: Must be an integer from 10 to 3600.
**ignore response-port-validation**

This keyword is available in releases 8.1 and higher.
Default: disabled. To reset the default for this parameter, you must enter the following command:

```
no gtpc ignore response-port-validation
```

This keyword instructs the SGSN to ignore the response port validation.
For the SGSN to process incoming GTP responses to an incorrect port,
- this keyword must be entered, and
- the same `bind address` must be configured for GTPC and GTPU in the SGTP service.

**max-retransmissions num**

Default: 4
Configures the maximum number of retries for packets.
`num`: Must be an integer from 0 to 15.

**retransmission-timeout seconds**

Default: 5
Configures the control packet retransmission timeout in GTP, in seconds.
`seconds`: Must be an integer value from 1 through 20.

**send { common-flags | rab-context }**

- `common-flags`: This option configures the SGTP service to include or exclude the common flags IE during an Inter-SGSN RAU. When selected, the default is to send the common flags IE.
- `rab-context`: This option configures the SGTP service to include/exclude the radio access bearer (RAB) context IE in SGSN ‘context response’ message during Inter-SGSN Routing Area Update procedure. Default is to send the RAB context IE.

**Usage**

Use this command to configure GTP-C settings for the current SGTP service.

**Example**

Following command excludes the radio access bearer (RAB) context IE in the SGSN Context Response message during the inter-SGSN RAU procedure:

```
no gtpc send rab-context
```
gtpu

This command configures the GPRS Tunneling Protocol user data plane parameters (GTP-U) for this SGTP service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
gtpu { bind address ip_address | echo-interval | max-retransmissions | retransmission-timeout } +
```

```
no gtpu { bind | echo-interval }
```

```
default gtpu { echo-interval | max-retransmissions | retransmission-timeout }
```

**no**
Removes the configuration for the specified parameter from the current SGTP service configuration.

**default**
Resets the specified GTP-U parameter to its factory default.

**bind address ip_address**
Defines the GTP-U Gn interface IP address that binds to this SGTP service. The gtpu and the gtpc commands should be configured with the same bind address.

**echo-interval seconds**
Default: 60
Configures the echo interval.

```
seconds: Must be an integer from 60 through 3600.
```

**max-retransmissions num**
Default: 4
Configures the maximum number of retries for packets.

```
um: Must be an integer from 0 through 15.
```

**retransmission-timeout seconds**
Default: 5
Configures the retransmission timeout of packets, in seconds.

```
seconds: Must be an integer from 1 through 20.
```

**Usage**
Use this command to configure the GTP-U settings for the SGTP service.
Example

gtpu echo-interval 5
path-failure

This command specifies the method for determining if path failure has occurred.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
path-failure detection-policy gtp type
no path-failure detection-policy

no
  Deletes the path-failure definition from the configuration.

detection-policy gtp type
  Default: echo (for both GTPC and GTPU)
  Specifies the policy to be used, value options include:
  * `echo` - When set to `echo`, path failure is detected when the retries of echo messages time out.
  * `non-echo` - When set to `non-echo`, path failure is detected when the retries of non-echo messages time out.
```

**Usage**

Use this command to define the policy to detect gtp path failure.

**Example**

```
path-failure detection-policy gtp echo
```
pool

This command enables the default SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identify request messages.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

pool { default-sgsn | hop-counter count }

default pool hop-counter

no pool { default-sgsn | hop-counter }

default
Removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

no
Disables the default SGSN pooling functionality or removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

default-sgsn
Enables default SGSN pooling functionality for this SGSN.

hop-counter count
Default: 4
Enables and configures the SGSN pool hop-counter to set the number of hops and to include the configured count in the new SGSN Context Requests or the new SGSN Identify Requests.
If default-sgsn is enabled, then any messages relayed will have the default value of 4 for the counter if the message does not include this hop-counter ID.

count : Must be an integer from 1 to 255.

Usage
Use this command to enable the default flex functionality without exposing the pool (flex) structure. This functionality provides a means for SGSNs outside of the pool to reach a pooled SGSN on the basis of its NRI. Once the pooling has been enabled. Repeat the command using the hop-counter keyword to enable inclusion of the hop-counter IE in SGSN context/identify request messages and to configure the count for the pooling hop-counter. If the SGSN is behaving as the ‘default SGSN’, this SGSN will forward (relay) requests with the hop-count included to the target SGSN.

Example
Enable the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:
pool default-sgsn

Set the hop-count to be included in messages to 25:

pool hop-count 25
Chapter 192
S-GW Service Configuration Mode Commands

The S-GW (Serving Gateway) Service Configuration Mode is used to create and manage the relationship between an eGTP service used for either ingress or egress control plane and user data plane network traffic.
accounting context

Configures the GTPP accounting context and group selection for S-GW service.

Product
S-GW

Privilege
Administrator

Syntax

accounting context name [ gtpp group name ]

no accounting context

Usage

Use this command to specify the accounting context and/or GTPP accounting group the S-GW service will use to perform GTPP accounting.

Example

The following command specifies a GTPP accounting context named acct-2 and a GTPP accounting group named gtpp-grp-3 as the context and group the S-GW service will use:

    accounting context acct-2 gtpp group gtpp-grp-3
**associate**

Associates the S-GW service with QoS and policy control and charging configurations.

**Product**  
S-GW

**Privilege**  
Administrator

**Syntax**

```bash
associate { accounting-policy name | egress_proto { gtp | gtp-pmip | pmip } [ egress-context name [ egtp-service name ] [ mag-service name ] ] | ims-auth-service name | ingress egtp-service name | qci-qos-mapping name }

no associate { accounting-policy name | egress_proto [ egress-context [ egtp-service ] [ mag-service ] ] | ims-auth-service name | ingress egtp-service | qci-qos-mapping name | }
```

**no**  
Removes the specified association from the S-GW service.

**accounting-policy name**

Associates the S-GW service with an accounting policy configured in the same context. `name` must be an existing accounting policy and be from 1 to 63 alpha and/or numeric characters.

Accounting policies are configured through the `policy accounting` command in the Context Configuration Mode.

**egress_proto { gtp | gtp-pmip | pmip } [ egress-context name [ egtp-service name ] [ mag-service name ] ]**

Associates and configures the egress protocol for this S-GW service.

- `gtp`: Specifies that GTP is to be used for the S-GW service egress.
- `gtp-pmip`: Specifies that either GTP or PMIP is to be used for the S-GW service egress.
- `pmip`: Specifies that PMIP is to be used for the S-GW service egress.

**egress-context name**: Specifies that the context in this keyword is to be used for the S-GW service egress. `name` must be an existing context on this system and be from 1 to 63 alpha and/or numeric characters.

**egtp-service name**: Specifies that the service in this keyword is to be used for the S-GW service egress. `name` must be an existing eGTP service on this system and be from 1 to 63 alpha and/or numeric characters.

**mag-service name**: Specifies that the service in this keyword is to be used for the S-GW service egress. `name` must be an existing MAG service on this system and be from 1 to 63 alpha and/or numeric characters.

**ims-auth-service name**

Associates the S-GW service with an IMS authorization service configured in the same context. `name` must be an existing IMS auth service and be from 1 to 63 alpha and/or numeric characters.

IMS authorization services are configured through the `ims-auth-service` command in the Context Configuration Mode.
### ingress egtp-service name
Associates and configures the eGTP service ingress for this S-GW service. name must be an existing eGTP service on this system and be from 1 to 63 alpha and/or numeric characters.

### qci-qos-mapping name
Associates the S-GW service with QCI to QoS mapping parameters. name must be an existing QCI-QoS mapping configuration and be from 1 to 63 alpha and/or numeric characters. QCI-QoS mapping is configured through the **qci-qos-mapping** command in the Global Configuration Mode.

### Usage
Use this command to select a pre-configured QoS mapping and/or policy control and charging configuration to be used by the S-GW service.

### Example
The following command associates the S-GW service with an IMS authorization service named *ims-23*:

```
associate ims-auth-service ims-23
```
egtp-service

Configures an eGTP service to use as either an ingress (S1-U) or egress (S5/S8) service for the S-GW.

**Product**
S-GW

**Privilege**
Administrator

**Syntax**

```
egtp-service { egress { context name | service name } | ingress service name }
no egtp-service { egress { context | service } | ingress service }
```

**no**
Removes the selected EGTP service from this service.

```
egtp-service { context name | service name }
```

Specifies the egtp-service to be used as the egress eGTP service on a GTP based S5/S8 interface.

- **context name**: Specifies the name of the context where the eGTP service resides. *name* must be from 1 to 63 alpha and/or numeric characters and be an existing context name where an eGTP service resides.

- **Caution**: context name is not supported in this release.

```
service name
```

Specifies the name of the egress eGTP service. *name* must be from 1 to 63 alpha and/or numeric characters and be an existing eGTP service name.

```
ingress service name
```

Specifies the egtp-service to be used as the ingress eGTP service on the S11 interface. *name* must be from 1 to 63 alpha and/or numeric characters and be an existing eGTP service name.

**Usage**

Use this command to configure the eGTP service to use with this S-GW service. The eGTP service must be existing and be configured with the appropriate parameters supporting the intended service type.

**Example**
The following command configures the S-GW service to use an eGTP service named *slu-egtp* as it’s ingress service:

```
egtp-service ingress service slu-egtp
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
- All

**Privilege**
- Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
```exit```

Usage
Return to the previous mode.
gtpu-error-ind

Configures the actions to be taken upon receiving a GTP-U error indication from an eNodeB or P-GW.

**Product**
S-GW

**Privilege**
Administrator

**Syntax**

```plaintext
  gtpu-error-ind { s1u { local-purge | page-ue [ custom1-behavior ] } | s5u { local-purge | signal-peer } }

  default gtpu-error-ind { s1u | s5u }
```

**default**

Rests the command to the default action for the specified interface. For S1-U, **page-ue** is the default action. For S5-U, **local-purge** is the default action.

**s1u { local-purge | page-ue [ custom1-behavior ] }**

Specifies the action to take when a GTP-U error indication is received from an eNodeB over the S1-U interface.

- **local-purge**: The S-GW clears the affected bearer (or PDN if error-ind is received on default bearer) locally without informing peer.
- **page-ue [ custom1-behavior ]**: The S-GW moves the complete UE state to S1-Idle and starts paging for this UE. If the custom1-behavior option is specified, the S-GW will guard the paging attempt with a timer of 60 seconds. Within this time the bearer must have the eNodeB TEID refreshed by an MME. Otherwise, the S-GW will clear the affected bearer with signaling. This is the default action for GTP-U error indication messages received on the S1-U interface.

**s5u { local-purge | signal-peer }**

Specifies the action to take when a GTP-U error indication is received from a P-GW over the S5-U interface.

- **local-purge**: The S-GW clears the affected bearer (or PDN if error-ind is received on a default bearer) locally without informing the peer. This is the default action for GTP-U error indication messages received on the S5-U interface.
- **signal-peer**: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:
  - For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
  - For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
  - The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

**Usage**

Use this command to specify the action to taken upon receiving a GTP-U error indication from either an eNodeB across an S1-U interface or from a P-GW across an S5-U interface.
Example
The following command sets the action to take upon receipt of a GTP-U error indication from the eNodeB to clear affected bearer:

```
gtpu-error-ind slu local-purge
```
mag-service

Identifies the Mobile Access Gateway (MAG) egress service through which calls are to be routed for this S-GW service.

**Product**
S-GW

**Privilege**
Administrator

**Syntax**

```
mag-service egress service name
no mag-service egress service
```

**no**
Removes the configured MAG egress service from this service.

```
no egress service name
```

Specifies the MAG service name to be used as the egress MAG service on a PMIP based S5/S8 interface. *name* must be an existing MAG service and be from 1 to 63 alpha and/or numeric characters.

**Usage**
Use this command to specify the name of the MAG service where calls are to be routed.

**Example**
The following command specifies that an existing MAG service named *mag3* is to be used to route call through for this S-GW service:

```
mag-service egress service mag3
```
path-failure

Configures the action to take upon the occurrence of a path failure between the S-GW and the MME, P-GW, or eNodeB.

Product
S-GW

Privilege
Administrator

Syntax

    path-failure { s11 | s1u | s5 | s5u } { local-purge | signal-peer }

    default path-failure { s11 | s1u | s5 | s5u }

    default
    Returns the command to the default setting of “local purge” for the selected interface.

{ s11 | s1u | s5 | s5u }

Specifies the interface to which the action will be applied.

s11: Indicates that the path failure action is to be applied to the S11 interface between the S-GW and the MME.

s1u: Indicates that the path failure action is to be applied to the S1-U interface between the S-GW and the eNodeB.

s5: Indicates that the path failure action is to be applied to the S5 interface between the S-GW and the P-GW.

s5u: Indicates that the path failure action is to be applied to the S5-U interface between the S-GW and the P-GW.

{ local-purge | signal-peer }

Specifies the action to apply to the selected interface.

local-purge: The S-GW clears the affected bearer (or PDN if path failure is received on a default bearer) locally without informing the peer. This is the default action for all interfaces.

signal-peer: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.

- For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.

- The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

Usage

Use this command to specify the type of action to take when a path failure occurs on one of the supported interfaces.

Example
The following command sets the path failure action for the S5 interface to “signal peer”:

```
path-failure s5 signal-peer
```
Chapter 193
SMS Service Configuration Mode Commands

The SMS (short message service) Service configuration mode is used to configure properties of the SMS Service component. The SGSN uses the SMS Service component to communicate via the Gd interface with a gateway message service controller (GMSC) to send short text messages (up to 140 octets in length) to a mobile (SMS-MT) and/or receive messages from a mobile (SMS-MO).

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

Enables the SGSN to send and/or receive cp-data (text messages).

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

cp-data max-retransmission retries_num

default cp-data max-retransmissions

<table>
<thead>
<tr>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use this command to configure the number of times the SGSN will attempt to retransmit a message.</td>
</tr>
</tbody>
</table>

Example

cp-data max-retransmission 2
mo-message-forwarding-destination

This command defines the SGSN’s handling policy for MO (mobile originating) message.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ default ] mo-message-forwarding-destination { gmsc-selected-from-imsi | smsc-supplied-by-subscriber }

---

default

Resets the SMS service configuration to the default message forwarding technique.

---

gmsc-selected-from-imsi

Entering this keyword enables SMS-MO messages to be forwarded on the basis of their IMSI prefix.

---

smsc-supplied-by-subscriber

Entering this keyword enables SMS-MO messages to be forwarded on the basis of the SMSC (SMS controller) address provided by the subscriber.

---

Usage

Use this command to define how the mobile originated SMS are to be routed.

---

Example

mo-message-forwarding-destination gmsc-selected-from-imsi
smsc-routing

This command configures the routing to the SMSC.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[ no ] smsc-routing { { any | imsi-starts-with | msisdn-starts-with } { isdn isdn_number | mobile-global-title mgt_number | point-code pt_code } }

any
Configures routing according to any IMSI prefix.

imsi-starts-with IMSI_prefix
Defines the IMSI prefix. Enter a string of up to 15 integers.

msisdn-starts-with msisdn_prefix
Defines the MSISDN prefix. Enter a string of up to 15 integers.

isdn isdn_number
Defines the ISDN E.164 number of the SMSC.

mobile-global-title mgt_number
Defines the mobile global title for conversion

point-code pt_code
Defines the point code for the SMSC. Enter a string of up to 11 digits in SS7 dotted decimal or decimal format

Usage

Use this command to define routing to the SMSC based on any point code.

Example

smsc-routing any point-code 1.222.1
timeout

This command defines the SMS service timers.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
timeout { tc1n-timer | tr1n-timer time | tr2n timer time }

default timeout { tc1n-timer | tr1n-timer | tr2n timer }
```

**default**
Resets the configuration to the default value for the specified timer.

**tc1n-timer time**
Configures the TC1N timer in seconds.
*time*: Must an integer from 1 to 255. The default is 5 seconds.

**tr1n-timer time**
Configures the TR1N timer in seconds.
*time*: Must an integer from 1 to 255. The default is 30 seconds.

**tr2n-timer time**
Configures the TR2N timer in seconds.
*time*: Must an integer from 1 to 255. The default is 30 seconds.

Usage
Use this command to set SMS service timers. The command can be repeated to set all of the timers, one-at-a-time.

Example
```
tr1n-timer 25
```
Chapter 194
SS7 Routing Domain Configuration Mode Commands

The SS7 Routing Domain configuration mode is used to configure Signaling System 7 (SS7) parameters. For convenience in configuration management, all SS7 parameters have been collected into a proprietary grouping called an SS7 routing domains.

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

This command creates or removes an M3UA Application Server Process (ASP) instance and enters the ASP configuration mode. See the SGSN ASP Configuration Mode chapter in the Command Line Interface Reference for command details.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```plaintext
asp instance asp_inst
no asp instance asp_inst
default asp instance asp_inst end-point port
```

- **no**
  Deletes the ASP instance for the SS7 routing domain configuration.

- **default**
  Sets the ASP instance parameters to the end-point port value of 2905.

- **instance asp_inst**
  Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.
  *asp_inst*: Must be an integer from 1 through 4.

Usage

Use this command to create an ASP instance or enter the ASP configuration mode.

Example

The following command enters the ASP configuration mode for a specific ASP.

```plaintext
asp instance 1
```
description

This command defines an alphanumeric string that describes the current SS7 routing domain. This is used for operator reference only.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

description string
no description

no
Removes the description string from the current SS7 routing domain configuration.

string
Specifies the alphanumeric string that is stored. Strings with spaces must be enclosed in double-quotes (see the example below).
string: Must be from 1 to 255 alphanumeric characters.

Usage
Use this command to set a description for reference by operators.

Example
The following command sets the description to identify a routing domain for messages transmitted within a national boundary.

description "National Service Routing Domain"
end

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

**Product**
SGSN, HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
exit
```

**Usage**

Return to the Exec mode from any configuration mode.
exit

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

**Product**
SGSN, HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the previous configuration mode.
inbound-asp-identifier validate

This command enables validation of ASP identifiers inbound to the SGSN via routes defined with this SS7 routing domain.

**Important:** This command is only available in releases 8.1 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
inbound-asp-identifier validate
```

[ default | no ] inbound-asp-identifier validate

**Usage**
The standard is to validate the ASP Id. However, in some circumstances it is necessary to skip such validation. For example, if the same ASP Id is assigned to more than one RNC (peer-server).

**Example**
Use the following command to skip validation of inbound ASP Ids:

```
no inbound-asp-identifier validate
```

Use either of the following commands to enable validation if it has been disabled:

```
default inbound-asp-identifier validate
inbound-asp-identifier validate
```
linkset

This command creates an instance of an MTP3 linkset and enters the linkset configuration mode. See the Linkset Configuration Mode chapter in Command Line Interface Reference for the commands to configure the linkset.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
linkset id id
no linkset id id

no
Removes the identified linkset definition from the system configuration.

id
This value uniquely identifies a linkset for the specific SS7 routing domain.
$id$: Must be an integer of 1 to 49.
```

Usage

This command creates instances of linkset configurations and provides access to the linkset configuration mode.

Example

Use the following command to create the 12th linkset:

```
linkset id 12
```
MTU-size

This command has been deprecated.
**peer-server**

This command creates a peer-server instance to setup a SIGTRAN peer for sending and receiving M3UA traffic. Completing the command automatically enters the peer-server configuration mode. To define 1 or more (up to 145) peer servers, use the commands documented in the *Peer-Server Configuration Mode* chapter in this reference.

**Product**
SGSN, HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
peer-server id srvr_id
no peer-server id srvr_id
```

- **no**
  Removes the identified peer-server definition from the system configuration.

- **srvr_id**
  srvr_id uniquely identifies a peer-server. The id must be an integer from 1 to 49.

**Usage**

Use the following command to create a definition for peer-server 2 and enter the configuration mode to configure the communication parameters for peer-server 12.

**Example**

```
peer-server id 12
```
route

This command configures SS7 routes for the current SS7 routing domain.

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```plaintext
route destination-point-code dp_code { linkset id id [ priority pri_value ] | peer-server-id srvr_id }

no route destination-point-code dp_code { linkset id id | peer-server-id srvr_id }
```

**no**
Removes the SS7 route from the current SS7 routing domain configuration.

**destination-point-code dp_code**
Specifies the SS7 destination point code for this route.
Reminder: the point-code structure must match the variant defined for the SS7 routing domain when the SS7RD was configured in the global configuration mode.

**linkset id id**
This keyword identifies a linkset instance, created and configured with the `linkset` command.
This keyword identifies a linkset instance, created and configured with the `linkset` command.
`id`: Must be an integer from 1 to 49.

**peer-server-id srvr_id**
This keyword identifies a peer-server configuration instance, created and configured with the `peer-server` command.
`srvr_id` must be an integer from 1 to 49.

**Usage**
This command associates the previously configured linksets and peer servers and the destination point codes with a specified SS7 route.

**Example**
Define a route setting an ITU-type destination point-code address for the linkset Id 12:

```plaintext
route destination-point-code 6.211.6 linkset id 12
```
**routing-context**

Identifies the routing context for this SS7 routing domain.

**Product**
SGSN, HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
routing-context value
```

```
default routing-context
```

```
default
```

Resets the local routing context value to the index (instance ID) for this SS7 routing domain.

```
value
```

An integer that uniquely identifies the routing context for this SS7 routing domain.

**value:** Must be integers from 1 to 65535 (for releases 8.0) or 1 to 4294967295 (for releases 8.1 and higher).

**Usage**

Use this command to set the routing context IDs for a specific SS7 routing domain configuration.

**Example**

```
routing-context 2355
```
ssf

This command sets the network indicator in the subservice field for SS7 message signal units (MSUs).

Product
SGSN, HNB-GW

Privilege
Security Administrator, Administrator

Syntax

```
ssf ( international | national | reserved | spare )
```

- **international**
The network indicator identifies the message as international with a point code structure that does not match the national point code structure.

- **national**
The network indicator identifies the messages as having a national point code structure.

- **reserved**
Provides an alternate network indicator for national messages.

- **spare**
Provides an alternate network indicator for international messages.

Usage

In SS7 signaling, the Message Transfer Part (MTP) Level 2 message signal units (MSUs) contain a service information octet (SIO). The SIO field in an MSU contains a 4-bit subservice field (SSF) followed by a 4-bit service indicator. The indicator carried in the message’s routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the nation - international. As well, the 4-bit SSF determines the point code structure of the messages transmitted from the SGSN.

Example

For messages being transmitted within a country, set the indicator to national with the following command.

```
ssf national
```
Chapter 195
SSH Configuration Mode Commands

The Secure Shell Configuration Mode is used to manage the SSH server options for the current context.
end

Exits the SSH server configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Administrator, Config-administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
**exit**

Exits the secure shell server configuration mode and returns to the context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the context configuration mode.
listen

This command configures the SSH server in the current context to only listen for connections from the interface with the specified IP address. The default behavior is to listen on all interfaces.

Product
All

Privilege
Security Administrator, Administrator

Syntax

\texttt{\textbf{listen} \textit{ip\_address}}

\textit{no \textbf{listen}}

\textit{no}

Disable listening for a specific interface address and enable listening on all interfaces.

Usage
Use this command to configure the SSH server for the current context to only listen for connections from the interface with the specified IP address. Only one IP address may be set for listening.

Example
The following command specifies that the Server should only listen for connections in the interface with the IP address of 192.168.0.10:

\texttt{listen 192.168.0.10}
**max servers**

Configures the maximum number of SSH servers that can be started within any 60 second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
max servers number
```

*number*

Default: 40

Specifies the maximum number of servers that can be spawned in any 60 second interval. number must be a value in the range from 1 to 100.

**Usage**

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true as well in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

**Example**

```
max servers 50
```
subsystem

Configures the system to perform file transfers using secure ftp (sftp) over ssh v2. Administrator users must be configured with the ftp attribute privilege to issue this command.

Product
All

Privilege
Security Administrator, Administrator

Syntax

subsystem { cli | sftp }
no subsystem { cli | sftp }

no
Disables either the sftp ssh file transfer method or disables access to the CLI over ssh.

cli
Default: Enabled
Configures the SSH system for the current context to allow access to the CLI.

sftp
Default: Disabled
Enables the SSH system for the current context to perform file transfers using secure ftp (sftp) over ssh v2.

Usage
Use this command to enable or disable file transfers using secure ftp over an ssh v2 tunnel. Also use this command to enable or disable access to the CLI over an SSH connection.

Example
The following command enables SFTP for the current context:

    subsystem sftp

The following command disables access to the CLI through an SSH session for the current context:

    no subsystem cli
Chapter 196
Subscriber Configuration Mode Commands

The Subscriber Configuration Mode is used to create local subscribers as well as to set default subscriber options for the current context.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          subscriber
            { default | name name }
              Subscriber Configuration Mode
```
aaa group

Configures a AAA server group for AAA functionality at the subscriber level.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] aaa group group_name

default aaa group

group_name
The AAA group to configure for authentication and/or accounting for the specific subscriber. 
group_name must be a string of length between one to 63 characters.

no
Disables the specified AAA group for the specific subscriber.

default
Sets/restores default AAA group specified at the context level or default subscriber profile.

Usage
Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for subscribers in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).

Example
The following command applies the AAA server group star1 to a subscriber within the specific context:

    aaa group star1

The following command disables the AAA group for the specific subscriber:

    no aaa group group_name
access-link ip-fragmentation

Configures IP fragmentation processing over the Access-link (\, GTP etc).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }
```

**df-ignore**

Default: Enabled
Ignore the DF bit setting. Fragment and forward the packet over the access link.

**df-fragment-and-icmp-notify**

Default: Disabled
Partially ignore the DF bit. Fragment and forward the packet, but also return an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to 1 ICMP error packet per second per session.

**normal**

Default: Disabled
Normal processing. Drop the packet and send an ICMP unreachable message to the source of packet. This is the default behavior.

**Usage**

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.

**Example**

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command: `access-link ip-fragmentation df-ignore`
# accounting-mode

This command sets the accounting mode for the current local subscriber configuration.

## Product
PDSN, HA, ASN GW, S-GW

## Privilege
Administrator

## Syntax

```
accounting-mode { flow-based | gtp [ radius-diameter ] | none | radius-diameter [ gtp ] | rf-style }
```

```
default accounting-mode
```

---

### default
Sets the type of accounting to be performed for the current local subscriber to the default setting.

Default: radius-diameter

### flow-based
Diameter flow-based accounting is enabled for the current local subscriber.

### gtp [ radius-diameter ]
GTPP CDR RADIUS accounting is enabled for the current local subscriber. The `radius-diameter` keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

### none
Accounting is disabled for the current local subscriber and no charging records will be generated.

### radius-diameter [ gtp ]
RADIUS-Diameter accounting is enabled for the current local subscriber. The `gtp` keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

### rf-style
Diameter Rf interface accounting is enabled for the current local subscriber.

## Usage
This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.

Use this command to enable or disable RADIUS/Diameter accounting for any subscribers that use the current local subscriber configuration.

If the `gtp` option is used, then GTTP RADIUS is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode and GTTP charging records will be enabled.

If the `radius-diameter` option is used, either the RADIUS or the Diameter protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.
RADIUS accounting can also be enabled and disabled at the context level with the `aaa accounting` command in the Context Configuration Mode. If RADIUS accounting is enabled at the context level, the `accounting-mode` command can be used to disable RADIUS accounting for individual local subscriber configurations.

If the accounting mode is set to `rf-style`, then BM will generate accounting records corresponding to AIMS RF.

**Example**

To disable accounting for the current subscriber, enter the following command:

```
accounting-mode none
```
active-charging bandwidth-policy

This command configures the bandwidth policy to be used for the subscriber.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
active-charging bandwidth-policy bandwidth_policy

{ default | no } active-charging bandwidth-policy
```

- **default**
  Specifies that the default bandwidth policy configured in the rulebase be used for this subscriber.

- **no**
  Disables bandwidth control for this subscriber.

- **bandwidth_policy**
  Specifies the bandwidth policy name.
  *bandwidth_policy* must be an alpha and/or numeric string from 1 through 63 characters in length.

Usage

Use this command to configure bandwidth policy to be used for subscribers.

Example

The following command configures a bandwidth policy named *standard* for the subscriber:

```
active-charging bandwidth-policy standard
```
active-charging rulebase

This command specifies the name of the rulebase to be used for this subscriber.

Product  
ECS

Privilege  
Security Administrator, Administrator

Syntax

active-charging rulebase rulebase_name

no active-charging rulebase

no

Removes the previously specified rulebase for the subscriber.

rulebase_name

Name of the specific active charging service rulebase.

rulebase_name must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage

This command specifies the name of the rulebase for specific subscriber (reals).

If the specified rulebase does not exist in the Active Charging service, the call will be rejected.

Example

Following command specifies the active charging rulebase rule1 for specified subscriber.

active-charging rulebase rule1
always-on

Once the idle timeout limit is reached, keep the current subscriber session connected as long as the subscriber is reachable.

⚠️ **Caution:** When always-on is enabled, the subscriber must have an idle time-out period configured (default is 0, no time-out). Failure to configure an idle time-out results in a subscriber session that is indefinite in length.

Two timers and a counter are associated with this feature. Refer to the `timeout` command in this chapter and the `ppp echo-retransmit-timeout msec` and `ppp echo-max-retransmissions num_retries` commands.

Default: Disabled.

**Product**
PDSN, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```markdown
always-on
no always-on

no
```

Disables `always-on`. The user is disconnected after the idle time expires.

**Usage**

If this parameter is enabled for a subscriber, when the idle time-out limit is reached the subscribers IP/PPP session remains connected as long as the subscriber is reachable. This is true even if the airlink between the mobile device and the RN (Radio Node) is moved from active to dormant (inactive) status. When the idle timeout limit is reached, the PDSN determines availability using LCP keepalive messages. A response to these messages indicates that the “always-on” status should be maintained. Failure to respond to a predetermined number of LCP keepalive messages causes the PDSN to tear-down (disconnect) the subscriber session.

**Example**

Enable always on for the current subscriber by entering the following command:

```markdown
always-on
```
asn-pdfid

This command configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Syntax

[ no ] asn-pdfid pdf_id asn-service-profile-id svc_profile_id asn-sdfid sdf_id

no
Removes/disables the configured identifiers for this subscriber in ASN-GW service.

asn-pdfid pdf_id
Specifies the an unique ASN Packet Data Flow identifier for this subscriber.
pdf_id must be an integer between 1 and 65535.

asn-service-profile-id svc_profile_id
Specifies an unique ASN Service Profile Identifier for this subscriber.
svc_profile_id is a preconfigured Service Profile Identifier configured in the Context Configuration Mode.

asn-sdfid sdf_id
Specifies the an unique ASN Service Data Flow identifier for this subscriber.
sdf_id must be an integer between 1 and 65535.

Usage
Use this command to configure subscriber profile for QoS parameters in an ASN-GW service.
A maximum of 4 QoS profiles can be configured for a subscriber.

Example
The following command configures the QoS profile for a subscriber as PDF id 1, Service Profile id 3, and Service Data Flow id 2:

asn-pdfid 1 asn-service-profile-id 3 asn-sdfid 2
asn-policy

This command configures the identifiers for packet data flow, service data flow, and service profile in an ASN GW service.

Product
ASN GW

Privilege
Security Administrator, Administrator

Syntax

asn-policy {classifiers downlink {strict | loose} | idle-mode {allow | disallow}}

[no | default] asn-policy idle-mode

[default] asn-policy classifiers downlink

no
Removes/disables the configured policy for this subscriber in ASN GW service.

default
Sets the ASN policy to default for this subscriber.
For downlink traffic classifier default policy is “loos” and for idle mode policy the default action is to allow idle mode operation in an ASN GW service.

idle-mode
Sets the idle mode policy for this subscriber in an ASN GW service.

allow
Default: enabled
Enables the policy for this subscriber to allow idle mode operation in an ASN GW service.

disallow
Default: disabled
Enable the policy for this subscriber to disallow idle mode operation in an ASN GW service.

classifiers downlink
Sets the classifier policy for all service flows coming from HA to FA for this subscriber’s matching classifier.

strict
Default: disabled
This option discards all the service flows coming from HA to FA and any other packets not matching to any of the classifiers set for this subscriber.
**loose**

Default: enabled

This option allows all the service flows coming from HA to FA and any other packet does not matching to any of the classifiers set for this subscriber and sent to the BS/MS over downlink flow.

**Usage**

Use this command to configure subscriber policy to allow/disallow the idle mode operation or the downlink traffic flow for a subscriber in an ASN GW service.

This command allows MS to transition to idle mode with an ASN GW.

**Example**

The following command configures the policy to allow the idle mode for an MS with an ASN GW:

```plaintext
default asn-policy idle-mode
```
authorized-flow-profile-id

When a profile ID is requested by the Mobile Node (MN), this command sets the value that is authorized by the AGW.

Product

PDSN, ASN GW

Privilege

Security Administrator, Administrator

Syntax

authorized-flow-profile-id profile_id direction { bidirectional | forward | reverse }

no authorized-flow-profile-id profile_id

---

no

Remove the existing profile ID setting specified by profile_id. profile_id must be an integer from 0 through 65535.

---

profile_id

The profile ID number that is authorized for the current subscriber. profile_id must be an integer from 0 through 65535.

---

direction { bidirectional | forward | reverse }

This specifies in which data direction the profile ID should be applied.
- bidirectional: This profile ID pertains to both the forward and reverse directions.
- forward: This profile ID pertains to data going to the MN.
- reverse: This profile ID pertains to data coming from the MN.

Usage

Use this command to set the profile ID that the AGW will authorize for a subscriber.

---

Example

Set the profile ID for both directions to 3 for the current subscriber by entering the following command

authorized-flow-profile-id 3 direction bidirectional
content-filtering category

This command enables/disables the specified preconfigured Category Policy Identifier for policy based Content Filtering support to the subscriber.

Product
All

Privilege
Security Administrator, Administrator

Syntax

content-filtering category policy-id cf_policy_id
no content-filtering category policy-id

no
Disables the configured category policy identifier for Content Filtering support to the subscriber. This is the default setting.

category policy-id cf_policy_id
This command applies the content filtering category policy ID, configured in Active Charging Configuration mode, to this subscriber. 

`cf_policy_id` must be a preconfigured category policy id in Active Charging Configuration Mode.
In case category policy identifier `cf_policy_id` used here is not configured in Active Charging Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

**Important:** Category Policy Id configured through this mode overrides the Category Policy id configured through `content-filtering category policy-id` command in Rulebase Configuration Mode of Active Charging Service Configuration mode.

Usage

Use this command to enter the Content Filtering Policy Configuration mode and to enable or disable the Content Filtering Category Policy ID for a Subscriber.

**Important:** If Content Filtering Category Policy ID is not specified here the similar command in Rulebase Configuration Mode of Active Charging Configuration Mode determines the policy.

Up to 64 different policy identifier can be defined in a Content Filtering support service.

Example

Following command enters the Content filtering Policy Configuration mode and enables the Category Policy Id 101 for Content Filtering support.

```
content-filtering category policy-id 101
```
**cscf core-service**

CSCF/A-BG core service that maps to the current domain.

**Product**
SCM (CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Syntax**

```
cscf core-service name name
no cscf core-service
```

**cscf core-service name name**

Specifies the name of the CSCF/A-BG core service. _name_ must be from 1 to 63 alpha and/or numeric characters.

**no cscf core-service**

Removes the CSCF/A-BG core service from the domain.

**Usage**

Use this command to map a CSCF/A-BG core service to the current domain.

**Example**

The following command creates a CSCF core service named _cs1_:

```
cscf core-service name cs1
```

The following command removes the CSCF core service from this domain:

```
no cscf core-service
```
cscf county-name

Assigns a Last Routing Option (LRO) profile county name to the subscriber for finding the correct Public Safety Answering Point (PSAP) during emergency calls.

Product

SCM (S-CSCF)

Privilege

Security Administrator, Administrator

Syntax

[ no ] cscf county-name name

cscf county-name name

Specifies the LRO profile county name of the subscriber.

name must be an existing LRO profile county name and be from 1 to 127 alpha and/or numeric characters.

no

Removes the LRO profile county name from the subscriber.

Usage

Use this command to assign an LRO profile county name to the subscriber.

Example

The following command assigns county name norfolk to the subscriber:

    cscf county-name norfolk

The following command removes county name norfolk from the subscriber:

    no cscf county-name norfolk
**cscf nat-applicable**

Indicates if NAT (Network Address Translation) processing is required for this domain.

**Product**
SCM (CSCF/A-SBC)

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] cscf nat-applicable
```

```
no
Disables NAT processing for this domain.
```

**Usage**
Use this command to indicate whether NAT processing is required for this domain.

**Example**
The following command indicates NAT processing is required for this domain:

```
cscf nat-applicable
```

The following command disables NAT processing for this domain:

```
no cscf nat-applicable
```
cscf private-user-id

Assigns a private user identity to the subscriber.

**Product**
SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] cscf private-user-id user_id
```

- **no**
  Removed the private user identity of the subscriber.

- **cscf private-user-id user_id**
  Specifies the private user identity of the subscriber.
  *user_id* must be from 1 to 127 alpha and/or numeric characters.

**Usage**

Use this command to assign a private user identity to the subscriber.

**Example**

The following command assigns a private user identity named *user007* to the subscriber:

```
cscf private-user-id user007
```

The following command removes private user identity named *user007* from the subscriber:

```
no cscf private-user-id user007
```
cscf session-template

Assigns a CSCF session template to the subscriber profile.

Product
SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege
Security Administrator, Administrator

Syntax

```
cscf session-template name name
no cscf session-template
```

- `cscf session-template name name`
  Specifies the name of the CSCF session template.
  `name` must be an existing CSCF session template name and be from 1 to 79 alpha and/or numeric characters.

- `no cscf session-template`
  Removes the assignment of a session template to the subscriber profile.

Usage
Use this command to bind a CSCF session template to a subscriber profile.

Example
The following command assigns a CSCF session template named `template4` to the subscriber profile:
```
cscf session-template name template4
```

The following command removes the assignment of a session template to the subscriber profile:
```
no cscf session-template
```
data-tunneling ignore df-bit

This command controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for GRE, IP-in-IP tunneling used for the MIP data path. If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header. Default is enabled.

Product
PDSN, HA, FA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

data-tunneling ignore df-bit
no data-tunneling ignore df-bit

Usage
Use this command to configure a user so that during Mobile IP tunneling the DF bit is not ignored and packets are not fragmented.

Example
To disable fragmentation of a subscriber's packets over a MIP tunnel even when the DF bit is present, enter the following command:

no data-tunneling ignore df-bit
dcca origin host

Important: This command has been deprecated, and is replaced by the dcca origin endpoint command.
dcca origin endpoint

**Important:** This command is obsolete. To configure the Diameter Credit Control Origin Endpoint, in the Credit Control Configuration mode, use the `diameter origin endpoint` command.
dcca peer-select

Specifies the Diameter credit control primary and secondary peer for credit control.

Product
ECS

Privilege
Security Administrator, Administrator

Syntax

```
dcca peer-select peer host_name [ realm realm_name] [ secondary-peer host_name [ realm realm_name] ]
no dcca peer-select
```

no
Removes the previously configured Diameter credit control peer selection.

```
peer host_name
```
A unique name that you specify for the peer.
peer_name must be an alpha and/or numeric string of from 1 through 127 characters. peer_name allows punctuation marks.

```
secondary-peer host_name
```
Specifies a back-up host that is used for fail-over processing. When the route-table does not find an AVAILABLE route the secondary host performs a fail-over processing.

```
realm realm_name
```
The realm_name must be an alpha and/or numeric string of 1 through 127 characters in length. The realm may typically be a company or service name. realm_name allows punctuation characters.

Usage
Use this command to select a Diameter credit control peer and realm.

⚠️ WARNING: This configuration completely overrides all instances of diameter peer-select that have been configured with in the Credit Control Configuration Mode for an Active Charging service.

Example
The following command selects a Diameter credit control peer named test and a realm of companyx:

```
dcca peer-select peer test realm companyx
```
default

Restores the default value for the option specified for the current subscriber.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default {access-link ip-fragmentation|accounting-mode|data-tunneling
ignore df-bit|idle-timeout-activity dormant-downlink-data|inter-pdsn-handoff|ip {
alloc-method|allowed-dscp|header-compression|hide-service-address|
multicast discard|gqs-dscp|source-validation|loadbalance-tunnel-peers|
long-duration-action|mobile-ip|home-agent|mn-aaa-removal-indication|mn-
ha-hash-algorithm|reverse-tunnel|security-level|send {dns-address|
terminal-verification | } | permission | ppp | always-on-vse-packet|data-
compression {mode|protocols} | keepalive | min-compression-size | mtu } | radius
accounting interim interval-timeout | timeout {absolute|idle} }
```

**access-link ip-fragmentation**
Sets the method for fragmenting packets over the MN access link to its default of normal. Drop the packet and send ICMP unreachable to the source of packet.

**accounting-mode**
Enables Radius accounting for the current local subscriber configuration.

**data-tunneling ignore df-bit**
Sets this option to the default behavior, which is to send an *ICMP unreachable - need to frag* message back to the sender and drop the packet, in the case that fragmentation is required but the DF bit is set.

**idle-timeout-activity dormant-downlink-data**
Sets this option to the default behavior. When downlink data packets are transmitted to the Mobile node and the session is in dormant mode the session idle timer is reset.

**inter-pdsn-handoff**
During a handoff from one PDSN to another, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address the PDSN will not disconnect the session immediately. The PDSN tries to assign the proposed address of the session in the IPCP configuration NAK.

```
ip { | allowed-dscp | header-compression | hide-service-address |
multicast discard | gqs-dscp | source-validation | user-datagram-tos copy }
```

**allowed-dscp**: resets the allowed DSCP parameters to the system defaults: class none, max-class be.

**hide-service-address**: specifies the default setting for hide the ip-address of the service from the subscriber. Default is Disabled
multicast discard: configures the default multicast settings which is to discard PDUs
qos-dscp: sets the quality of service setting to the system default.
source-validation: Specifies the default IP source validation. Default is Enabled.
user-datagram-tos copy: Disable copying of the IP TOS octet value to all tunnel encapsulation IP headers.

loadbalance-tunnel-peers
Sets the tunnel load balancing algorithm to the system default.

long-duration-action
Sets the action that is taken when the long duration timer expires to the default: detection.

mobile-ip { home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm | reverse-tunnel | security-level | send { dns-address | terminal-verification } }
allow-aaa-address-assignment: Disables the FA from accepting a home address assigned by an AAA server.
home-agent: Sets home agent IP address to its default of 0.0.0.0.
match-aaa-assigned-address: Disables the FA validating the home address in the RRQ against the one assigned by AAA server.
mn-aaa-removal-indication: Sets this parameter to its default of disabled.
mn-ha-hash-algorithm: Sets the encryption algorithm to the default of hmac-md5.
reverse-tunnel: Sets this parameter to its default of enabled.
security-level: Sets this parameter to its default of none.
send dns-address: Disables the HA from sending the DNS address NVSE in the RRP.
send terminal-verification: Disables the FA from sending the terminal verification NVSE in the RRQ.

permission
Restores the subscriber’s service usage defaults.

ppp { always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation | keepalive | min-compression-size | mtu }
Sets the point-to-point protocol option defaults.
always-on-vse-packet: Re-enables the PDSN to send special 3GPP2 VSE PPP packets to the Mobile Node with a max inactivity timer value for always on sessions. This configuration is applicable only for PDSN sessions.
data-compression { mode | protocols }: restores the default value for either the data compression mode or compression protocols as follows:
  ● mode stateless
  ● all protocols enabled
ip-header-compression negotiation: sets the IP header compression negotiation to the system default: force.
keepalive: sets the subscriber’s PPP keep alive option to the system default: 30 seconds.
min-compression-size: restores the PPP minimum packet size for compression: 128 octets.
mtu: sets the maximum message transfer unit packet size to the system default: 1500 octets.
**radius accounting interim interval-timeout**
Disables the RADIUS accounting interim interval for the current subscriber.

**timeout [ absolute | idle | long-duration ]**
When a keyword is entered, this command resets the specified timeout to the system default: 0. When no keyword is specified, all timeouts are reset to the system defaults: 0.

**Usage**
Reset subscriber data to the system defaults. This is useful in setting the subscriber back to the basic values to possibly aid in trouble shooting or tuning a subscriber’s access and options.

**Example**
default ipqos-dscp
default permission
default data-compression mode
**dns**

Configures the domain name servers for the current subscriber.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] dns { primary | secondary } ip_address
```

- **no**
  Indicates the IP address is to be removed as either a primary or secondary domain name server.

- **primary | secondary**
  - **primary**: Indicates the primary domain name server for the subscriber is to be updated.
  - **secondary**: Indicates the secondary domain name server for the subscriber is to be updated.

- **ip_address**
  Specifies the IP address of the domain name server.

**Usage**
Set the subscriber DNS server lists as not all users will have the same set of servers.

**Example**

dns primary 1.2.3.4
no dns primary 1.2.3.4
dns secondary 1.2.5.6
no dns secondary 1.2.5.6
This command specifies the lifetime for a master session key (MSK) for extensible authentication protocol (EAP) authentication.

**Product**
ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[default] eap msk-lifetime dur
```

<table>
<thead>
<tr>
<th>Context</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets the lifetime duration to default value of 3600 seconds for master session key.</td>
</tr>
</tbody>
</table>

```
msk-lifetime dur
```

Specifies the lifetime duration on Master session key (MSK) in seconds for a WiMAX subscriber EAP authentication.

`dur` is the lifetime value in seconds and must be an integer from 60 through 65535.

**Usage**
This command is used to set the lifetime for MSK in EAP authentication for WiMAX subscriber.

**Example**
The following command sets the lifetime for MSK key to 4800 seconds for a WiMAX subscriber through EAP authentication:

```
eap msk-lifetime 4800
```
encrypted password

Designates use of password encryption.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
encrypted password password
```

*password*

*password* is the encrypted password and must be an alpha and/or numeric string of from 1 to 63 characters.

Usage

This command is normally used only inside configuration files.

Example

The following command sets an encrypted password of *qsf12d4*:

```
encrypted password qsf12d4
```
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the subscriber configuration mode and returns to the context configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
external-inline-server

This is a restricted command.
**firewall policy**

*Important:* This command is only available in StarOS 8.0. In StarOS 8.1 and later, this configuration is available in the Rulebase Configuration Mode.

This command enables/disables Stateful Firewall support for the subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
firewall policy firewall-required
{ default | no } firewall policy
```

- **no**
  Disables Stateful Firewall support for this subscriber.

- **default**
  Configures the default setting for Stateful Firewall support.
  Default: Disabled

- **firewall-required**
  Enables Stateful Firewall support for this subscriber.

**Usage**

Use this command to enable or disable Stateful Firewall support for this subscriber.

*Important:* Unless Stateful Firewall support for this subscriber is enabled using this command, firewall processing for this subscriber is disabled.

*Important:* If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

**Example**

The following command enables Stateful Firewall support for this subscriber:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for this subscriber:
no firewall policy
fw-and-nat policy

**Important:** This command is customer-specific and is only available in StarOS 8.1. This command must be used to configure the Policy-based Firewall-and-NAT feature.

This command configures the Firewall-and-NAT policy for the subscriber.

**Product**

FW, NAT

**Privilege**

Security Administrator, Administrator

**Syntax**

```
fw-and-nat policy fw_nat_policy
{ default | no } fw-and-nat policy
```

- **default**
  
  Specifies that the default Firewall-and-NAT policy configured in the rulebase be used for the subscriber.

- **no**
  
  Disables Firewall and NAT processing for the subscriber.

- **fw_nat_policy**
  
  Specifies the Firewall-and-NAT policy for the subscriber. `fw_nat_policy` must be an alpha and/or numeric string of 1 through 63 characters in length. Note that this policy will override the default `Firewall-and-NAT policy` configured in the ACS rulebase.

**Usage**

Use this command to configure the Firewall-and-NAT policy for subscribers. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be applied.

**Example**

The following command configures a Firewall-and-NAT policy named `standard` for the subscriber:

```
fw-and-nat policy standard
```
idle-timeout-activity

Defines whether downlink (towards Mobile Node) data packets transmitted when the session is dormant is treated as activity for the idle-timer (inactivity timer).

By default, downlink data transmitted over a dormant session restarts the idle-timer for that session (it is treated as activity for the session).

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] idle-timeout-activity dormant-downlink-data

no

Dormant mode downlink data is not treated as activity for the session idle-timer. The session idle timer is not reset.

Usage
Use this command to disable or re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode.

Example
Use the following command to disable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

idle-timeout-activity dormant-downlink-data

Use the following command to re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

no idle-timeout-activity dormant-downlink-data
**ims application-manager**

Specifies the application manager for the subscriber.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ims application-manager { domain-name domain-name | ipv4-address ipv4-address }
```

- **no**
  Disables the IMS application manager for this subscriber.

- **domain-name domain-name**
  Specifies the domain name of the application manager.
  `domain-name` must be from 1 to 63 alpha and/or numeric characters.

- **ipv4-address ipv4-address**
  Specifies the IPv4/IPv6 address of the application manager.

**Usage**
The ims application manager address is returned by HA to MN in DHCP Ack when it receives the DHCP inform from an AIMS subscriber.

**Example**

```
ims application-manager domain-name domain23
ims application-manager ipv4-address 192.168.23.1
```
**ims-auth-service**

It applies an IMS authorization service to a subscriber in a network access service (PDSN or GGSN service) for Gx/Ty interface support and functionality.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[default|no]ims-auth-service auth_svc_name
```

**default**

Sets / Restores default state of IMS authorization service, disabled or as specified at the context or network access service level or in subscriber template.

**no**

Disables the applied IMS authorization service for specific subscriber.

**auth_svc_name**

Specifies the name of IMS authorization service name that is used for Ty interface support for specific subscriber. `auth_svc_name` must be from 1 to 63 alpha and/or numeric characters preconfigured within the same context of this subscriber.

**Usage**

This feature provides the IMS authorization service configuration for Gx/Ty interface in IMS service node.

**Example**

Following command applies a previously configured IMS authorization service named `ims_interface1` to a subscriber within the specific context.

```
ims-auth-service ims_interface1
```
inter-pdsn-handoff

Configure the system to enforce the MN’s use of its assigned IP address during IPCP negotiations resulting from inter-PDSN handoffs.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] inter-pdsn-handoff require ip-address

no
Disables the rejecting of sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

Usage
This command is used to configure the system to reject sessions that are re-negotiating IPCP after an inter-PDSN handoff if the IP address they propose does not match the one initially provided by the PDSN. The session would be rejected even if the proposed address was 0.0.0.0. If this parameter is disabled, the PDSN will attempt to re-assign the IP address initially provided.

Example
To set the PDSN to not allow a mismatched IP address during a PDSN to PDSN handoff of a MIP call, use the following command:

    inter-pdsn-handoff require ip-address

To set the PDSN so that it will not disconnect the session immediately, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address after inter-pdsn handoff, use the following command:

    no inter-pdsn-handoff require ip-address
ip access-group

Configures IP access group for the current subscriber.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip access-group group_name [ in | out ]

no
Indicates the access group specified is to be cleared from the subscribers configuration.

group_name
Specifies the name of the IPv4/IPv6 access group. acl_group_name is a configured ACL group and must be an alpha and/or numeric string of 1 to 79 characters.

in | out
Default: both (in and out)
Specifies the access-group as either inbound or outbound by the keywords in and out, respectively. If neither of these key words is specified, the command associates the group_name access group with the current subscriber for both inbound and outbound access.

Usage
Set the subscriber access group to manage the access control for subscribers as a logical group.

Example
The following command associates the sampleGroup access group with the current subscriber for both inbound and outbound access:

ip access-group sampleGroup

The following removes the outbound access group flag for sampleGroup:

no ip access-group sampleGroup out
ip address

Configures a static IP address for use by the subscriber.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip address ip_address netmask

no
Removes a previously configured IP address assignment.

ip_address
The IP address assigned to the subscriber.

netmask
The subnet mask that corresponds to the assigned IP address.

Usage
Use this command to assign a static IP address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example
The following command configures a static IP address of 192.168.1.15 with a subnet mask of 255.255.255.0 to the subscriber:

ip address 192.168.1.15 255.255.255.0
ip address pool

Configures IP address pool properties for the subscriber.

Product
PDSN, GGSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip addresspool name pool_name

no
Removes a previously configured static address.

name pool_name
Specifies the IP address pool or IP address pool group from which the subscriber's IP address is assigned. pool_name must be the name of an existing IP pool or IP pool group and from 1 to 31 alpha and/or numeric characters.

Usage
Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to sessions from this subscriber. This command can be issued multiple times to specify multiple address pools for the subscriber. If multiple pools are specified, addresses are assigned for subscriber sessions from the pools based on the order in which the pools were configured. If an address can not be provided from the first-specified pool for whatever reason, the system attempts to assign an address from the second-specified pool, and so on. This operation is independent of the priorities configured for the pools. For example, if pool1 was specified for the subscriber first, and pool2 second, the system always attempts to assign addresses from pool1. If an address can not be assigned from pool1 (i.e. all addresses are in use), the system then attempts to assign an address from pool2.

Example
The following command configures the subscriber to receive IP addresses from an IP address pool named public1:

ip addresspool name public1
ip address secondary-pool

Configures secondary IP address pool properties for the subscriber to provide multiple IP host configuration behind one WiMAX CPE.

Product
ASN GW

Privilege
Security Administrator, Administrator

Syntax

```
ip address secondary-pool name aux_pool_name

no ip address secondary-pool name aux_pool_name
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a previously configured auxiliary pool named \texttt{aux_pool_name} for multiple host support in ASN GW service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>name aux_pool_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the secondary/auxiliary IP address pool or IP address pool group from which the IP address is assigned to host behind a WiMAX CPE having primary IP address. \texttt{pool_name} must be the name of an existing IP pool or IP pool group and from 1 to 31 alpha and/or numeric characters.</td>
</tr>
</tbody>
</table>

Usage

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to host behind a WiMAX CPE for multiple host session support. This command designates the IP address to secondary hosts from locally configured secondary IP address pool. To enable multiple host support behind a WiMAX CPE and configure maximum number of supported hosts use \texttt{secondary-ip-host} command in ASN Gateway Service Configuration mode.

Example

The following command configures the subscriber to receive IP addresses from a secondary IP address pool named \texttt{auxiliary} for secondary hosts behind the WiMAX CPE:

```
ip address secondary-pool name auxiliary
```
**ip allowed-dscp**

This command sets the Quality of Service (QoS) Differentiated Services (DiffServ) marking that a subscriber session is allowed. This is disabled by default.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ip allowed-dscp class classmax-class maxclass [rt-marking marking]
no ip allowed-dscp class
```

**no ip allowed-dscp class**

Resets the parameters to the defaults: class none, max-class be. This indicates that all packets are let through without any dscp checking

**class class**

This parameter specifies the Differentiated Services Codepoint (DSCP) class that the subscriber session may mark its packets with. If the subscriber sessions packets request a code point class higher than the code point class specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the `ip qos-dscp` command.

Default: none

*class* must be one of the following:
- a: packets with AF DSCPs are allowed
- e: packets with EF DSCPs are allowed
- o: packets for experimental or local use are allowed
- ao: packets with AF and EF DSCPs are allowed
- eo: packets with AF DSCPs or packets for experimental or local use are allowed
- ace: packets with EF DSCPs or packets for experimental or local use are allowed
- none: only the be and sc1 through sc7 codepoints are allowed

**max-class maxclass**

This parameter specifies the maximum code point that a subscriber session may mark its packets with. If the subscriber sessions packets request a code point higher than the code point specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the max-class and the `ip qos-dscp` command.

Default: none

*maxclass* must be one of the following:
- be, af12, af11, af22: are allowed. If a subscriber session marks its packets with anything after af22 in this list, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the maxclass and the `ip qos-dscp` command.
- only be, sc1 through sc7 codepoints are allowed. For example; if class is set to none and you set max-class be, only the be codepoints are allowed.

**Default:**

*maxclass* must be one of the following:
be: best effort forwarding
af13: assured Forwarding 13
af12: assured Forwarding 12
af11: assured Forwarding 11
af23: assured Forwarding 23
af22: assured Forwarding 22
af21: assured Forwarding 21
af31: assured Forwarding 31
af32: assured Forwarding 32
af33: assured Forwarding 33
af41: assured Forwarding 41
af42: assured Forwarding 42
af43: assured Forwarding 43
ef: expedited forwarding
sc1: selector class 1
sc2: selector class 2
sc3: selector class 3
sc4: selector class 4
sc5: selector class 5
sc6: selector class 6
sc7: selector class 7

**rt-marking**

This parameter is used for Mobile IP (MIP) reverse tunnels. When a MIP sessions packets do not have a DSCP marking, the Foreign Agent (FA) marks the packets with the value specified by **rt-marking**.

If the MIP sessions packets have a DSCP marking, the marking is subjected to the conformance rules for the values of class and max-class, then the final DSCP marking is copied from the inner IP header to the outer IP header.

Default: be

**marking** must be one of the following:
be: best effort forwarding
af11: assured Forwarding 11
af12: assured Forwarding 12
af13: assured Forwarding 13
af21: assured Forwarding 21
af22: assured Forwarding 22
af23: assured Forwarding 23
af31: assured Forwarding 31
af32: assured Forwarding 32
af33: assured Forwarding 33
af41: assured Forwarding 41
af42: assured Forwarding 42
af43: assured Forwarding 43
ef: expedited forwarding
sc1: selector class 1
sc2: selector class 2
sc3: selector class 3
sc4: selector class 4
sc5: selector class 5
sc6: selector class 6
**sc7**: selector class 7

**Usage**

Use this command to configure Quality of Service (QoS) for a subscriber session to allow a Differentiated Services (DiffServ) Code Point (DSCP) marker in the header of each IP packet that prompts network routers to apply differentiated grades of service to various packet streams.

This command uses `class` and type of marker (`rt-marking` for reverse tunnels) for configuration with `max-class` maximum code point that a subscriber session may mark its packets with.

**Example**

The following command will allow o packets for experimental or local use with best effort forwarding be:

```
ip allowed-dscp class o max-class be
```
ip context-name

Configures context to assign the subscriber to upon authentication. The context assigned to is considered the destination context which provides the configuration options for the services the subscriber is allowed to access.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip context-name name

no
Removes the current assigned context from the subscriber’s data.

name
Specifies the name of the context to assign the subscriber to once authenticated. name must be from 1 to 79 alpha and/or numeric characters.

Usage
Set the subscriber IP context to a common context when all subscribers from one or more contexts will use the same egress context.

Example

ip context-name sampleName
no ip context-name sampleName
**ip header-compression**

Configures the IP packet header compression options for the current subscriber. Although this command configures IP header compression algorithms, the IPCP negotiations determine when the header compression algorithm is applied.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip header-compression { rohc [ any [ mode { optimistic | reliable | unidirectional } ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr value | mrru value ] } | marked flows-only | max-hdr value | mrru value | downlink | uplink ] | vj }+ [ default | no ] ip header-compression
```

default
Restores this command’s default setting to the Van Jacobsen (VJ) header compression algorithm.

no
Disables all IP header compression.

```
rohc [ any [ mode { optimistic | reliable | unidirectional } ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr value | mrru value ] } } | marked flows-only | max-hdr value | mrru value | downlink | uplink ]
```

Specifies that the Robust Header Compression (ROHC) algorithms is used for data.

**Important:** ROHC is only supported for use with the PDSN.

**any**: Apply ROHC header compression in both the uplink and downlink directions.

**mode { optimistic | reliable | unidirectional }**:

- **optimistic**: Sets the ROHC mode to Bidirectional Optimistic mode (O-mode). In this mode packets are sent in both directions. A feedback channel is used to send error recovery requests and (optionally) acknowledgments of significant context updates from decompressor to compressor. Periodic refreshes are not used in the Bidirectional Optimistic mode.

- **reliable**: Sets the ROHC mode to Bidirectional Reliable mode (R-mode). This mode applies an intensive usage of a feedback channel and a strict logic at both the compressor and the decompressor that prevents loss of context synchronization between the compressor and the decompressor. Feedback is sent to acknowledge all context updates, including updates of the sequence number field.

- **unidirectional**: Sets the ROHC mode to Unidirectional mode (U-mode). With this mode packets are sent in one direction only, from the compressor to the decompressor. This mode therefore makes ROHC usable over links where a return path from the decompressor to the compressor is unavailable or undesirable.
CID-MODE { { LARGE | SMALL } [ MARKED-FLOWS-ONLY | DM | MAX-HDR value | MRRU value ] } Specifies the ROHC packet type to be used.

* LARGE | SMALL [ MARKED-FLOWS-ONLY | MAX-CID | MAX-HDR value | MRRU value ] Defines the ROHC packet type as large or small and optionally sets the following parameters for the packet type selected:

**MARKED-FLOWS-ONLY** Specifies that ROHC is to be applied only to marked flows.

**MAX-CID integer** Default: 0 The highest context ID number to be used by the compressor.

*integer* must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.

**MAX-HDR value** Specifies the maximum header size to use. Default: 168. *value* must be an integer from 0 through 65535.

**MRRU value** Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an integer from 0 through 65535.

MARKED-FLOWS-ONLY: Specifies that ROHC is to be applied only to marked flows.

MAX-HDR value: Specifies the maximum header size to use. Default: 168. *value* must be an integer from 0 through 65535.

MRRU value: Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an integer from 0 through 65535.

downlink: Apply the ROHC algorithm only in the downlink direction.

uplink: Apply the ROHC algorithm only in the uplink direction.

**Important:** When ROHC is enabled for downlink or uplink only the operational mode is Unidirectional.

**VJ**

Specifies that the VJ algorithm is used for header compression.

+ Either one or both of the keywords may be entered in a single command.

If both VJ and ROHC are specified, VJ must be specified first.

**Important:** If both VJ and ROHC header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

**Usage**

Header compression can be used to provide a higher level of security in IP traffic enhance bandwidth usage and lower bit errors.

By default the header compression algorithm is set to VJ.

**Example**

The following command disables all IP packet header compression:

no ip header-compression

The following command sets IP header compression to default VJ algorithm:

default ip header-compression

The following command also sets the IP header compression to the VJ algorithm:

ip header-compression vj
The following command enables the Internet Protocol Control Protocol (IPCP) to determine which protocol is the optimum algorithm for data in the downlink direction and use either VJ or ROHC as needed:

```
ip header-compression vj rohc
```

The following command enables ROHC for the downlink direction only:

```
ip header-compression rohc downlink
```

The following command enables ROHC in any direction using Bidirectional Optimistic mode:

```
ip header-compression rohc any mode Optimistic
```
**ip hide-service-address**

Hide the IP address of the service from the subscriber.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ip hide-service-address
```

- **no**
  Disable this command's function. This is the default behavior.

**Usage**

Use this command to prevent subscribers from using traceroute to discover the network addresses that are in the public domain and configured on services. This prevent users from pinging such addresses.

**Example**

To prevent subscribers from discovering IP addresses, enter the following command:
ip local-address

Configures the local-side IP address of the subscriber's point-to-point connection.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
ip local-address ip_address
no ip local-address
```

**Usage**
This parameter specifies the IP address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an "unnumbered" scheme for local-side addresses.

**Example**
The following command configures a local address of 192.168.1.23 for the MS:

```plaintext
local-address 192.168.1.23
```
ip multicast discard

Configures the IP multicast discard packet behavior.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip multicast discard

no

Removes a previously configured IP multicast discard.

Usage
This command specifies if IP multicast discard is enabled or disabled.

Example
The following command enables IP multicast discard for an APN:

ip multicast discard
**ip qos-dscp**

Configures quality of service options for the current subscriber using the differentiated services code point method. This is disabled by default.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ip qos-dscp option
no ip qos-dscp
```

`no`
Sets the quality of service option to its default value.

`option`
Default: be
Specifies the subscriber’s per hop quality of service setting as one of:
- `af11` (assured Forwarding 11)
- `af12` (assured Forwarding 12)
- `af13` (assured Forwarding 13)
- `af21` (assured Forwarding 21)
- `af22` (assured Forwarding 22)
- `af23` (assured Forwarding 23)
- `af31` (assured Forwarding 31)
- `af32` (assured Forwarding 32)
- `af33` (assured Forwarding 33)
- `af41` (assured Forwarding 41)
- `af42` (assured Forwarding 42)
- `af43` (assured Forwarding 43)
- `be` (best effort forwarding)
- `ef` (expedited forwarding)

**Usage**
Set the quality of service for a subscriber based upon the service level agreements.

**Example**

```
ip qos-dscp ef
no ip qos-dscp
```
Subscriber Configuration Mode Commands

ip qos-dscp
ip route

Configures the static route to use to reach the subscriber’s network.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ip route ip_address ip_mask [ gateway_address ]

no
Removes the configured route information from the subscriber data.

ip_address
Specifies the target IP address for which the route information applies.

ip_mask
Specifies the networking mask for the route.
1 bits in the ip_mask indicate that bit position in the ip_address must also have a value of 1.
0 bits in the ip_mask indicate that bit position in the ip_address does not need to match, i.e., the bit can be either a 0 or a 1.
For example, if the IP address and mask were specified as 172.168.10.0 and 255.255.255.224, respectively, the network mask will be 172.168.0.0 (obtained by logically ANDing the IP address with the IP mask).

gateway_address
Default: assigned remote IP address will be used as the gateway address.
Specifies the IP address of the next hop gateway for the route.

Usage
The static routes are also known as framed IP routes for subscribers. Static routes are typically applicable for subscribers connecting via other networks or when the mobile device acts as a gateway to a network on the far side of the device.
For example, if the mobile device is assigned IP address 1.2.3.4 and it acts as a gateway for the network 10.2.3.0 (with a network mask of 255.255.255.0) a static route would be configured with the ip_address being 10.2.3.0, ip_mask being 255.255.255.0, and gateway_address being 1.2.3.4.

Example

no ip route 1.2.3.4 1.2.3.0 0
no ip route 1.2.3.4 1.2.3.0 0 1.2.255.254
**ip source-validation**

Enables/disables packet source validation for the current subscriber. Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session. If an incorrect source address is received from the mobile node, the system attempts to renegotiate the PPP session. The parameters for IP source validation can be set by the `ip source-violation` command.

**Syntax**

```
[ no ] ip source-validation
```

- `no`
  - Disables source validation.

**Usage**

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

**Example**

The following command enables IP source validation:

```
ip source-validation
```

The following command disables IP source validation:

```
no ip source-validation
```
ip user-datagram-tos copy

This CLI controls copying of IP TOS octet value from IPv4/IPv6 datagrams to the IP header in tunnel encapsulation. This is disabled by default.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
ip user-datagram-tos copy [access-link-tunnel | both | data-tunnel]
no ip user-datagram-tos copy
```

- **no**
  Disable copying of the IP TOS octet value to all tunnel encapsulation IP headers.

- **access-link-tunnel**
  Copy the IP TOS octet value to the tunnel encapsulation IP header on the access side (RP) tunnel.

- **both**
  Use both access-link-tunnel and data-tunnel.

- **data-tunnel**
  Copy the IP TOS octet value to the tunnel encapsulation IP header on the MIP data tunnel or L3 tunnel (IP-in-IP, GRE).

Usage
Use this command to enable the copying of the IP TOS octet value to the tunnel encapsulation IP header. This functionality will enable PCF to detect special TOS marking in the outer IP header of A11 packets and to identify certain packets as QChat control messages. The BSC/PCF must give higher priority to QChat control messages.

Example
Enable copying of the IP TOS octet value to the tunnel encapsulation IP header for the access side tunnel by entering the following command;

```
ip user-datagram-tos copy access-link-tunnel
```

Disable copying of the IP TOS octet value to all tunnel encapsulation IP headers by entering the following command;

```
no ip user-datagram-tos copy
```
ip vlan

Configures subscriber-to-Virtual LAN (VLAN) associations.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

ip vlan

Syntax

ip vlan vlan-id
[ default | no ] ip vlan

default
Resets the vlan ID to the default setting.

no
Disables the vlan ID for the subscriber.

vlan-id
Is the vlan ID that is associated with the IP address for that session. vlan-id is an integer between 1 and 4094.

Usage
This command configures the subscriber vlan ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a vlan ID, then this subscriber configured vlan ID overrides it.

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

Example
Set the vlan ID to the default setting by entering the following command;

default ip vlan
**ipv6 access-group**

Configures the IPv6 access group for a subscriber.

**Product**

PDSN, GGSN, ASN GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
ipv6 access-group name [ in | out ]
```

**in**

Defines the access group as inbound.

**out**

Defines the access group as outbound.

**Usage**

Used to create an access group for a subscriber.

**Example**

The following command provides an example of an IPv6 access group with the name *list_1*:

```
ipv6 access-group list_1
```
ipv6 address

Configures a static IP address for use by the subscriber.

Product
PDSN, GGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] ipv6 address { prefix address | prefix-pool name }
```

no
 Deletes a previously configured ipv6 address.

prefix
 Specifies a static IPv6 address.

prefix-pool
 Specifies an IPv6 prefix pool name.

Usage
Use this command to assign a static IPv6 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example
The following command configures a static IP address of 1:1:1:1:1:1:1:1 with a length of 24 to the subscriber:

```
ipv6 address 1:1:1:1:1:1:1:1/24
```
ipv6 dns

Configures the IPv6 Domain Name Service (DNS) servers.

**Product**
PDSN, GGSN, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ipv6 dns { primary | secondary } {ipv6_dns_address}
```

- **no**
  Deletes a previously configured DNS server.

- **primary**
  Configures the primary DNS server for the subscriber.

- **secondary**
  Configures the secondary DNS server for the subscriber. Only one secondary DNS server can be configured.

- **ipv6_dns_address**
  Configures the IP address of the DNS server.

**Usage**

DNS servers are configured on a per subscriber basis. This allows each subscriber to use specific servers.

**Example**

The following command provides an example of setting the primary IPv6 DNS server:

```
ipv6 dns primary 1::1::1::1::1::1
```
### `ipv6 dns-proxy`

Configures the domain name server proxy for the current subscriber.

**Product**

PDSN, GGSN, ASN GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ default | no ] ipv6 dns-proxy
```

- **default**
  
  Disables the IPv6 DNs proxy functionality for a subscriber.

- **no**
  
  Removes the pre-enabled functionality of IPv6 DNS proxy for subscriber.

- **dns-proxy**
  
  Enables IPv6 DNS proxy functionality for a subscriber. If the functionality enabled, PDSN will act as a proxy DNS server.
  
  Default: disabled.

**Usage**

Used to enable/disable IPv6 DNS proxy for the subscriber. When enabled, the PDSN acts as a proxy DNS server for DNS IPv6 queries coming from the mobile station to the PDSN’s local PPP link address.

**Example**

The following command provides an example of disabling an IPv6 DNS proxy for the subscriber:

```
no ipv6 dns-proxy
```
ipv6 egress-address-filtering

Configures the egress address filtering for the subscriber.

Product
PDSN, GGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax

[ no ] ipv6 egress-address-filtering

no
Disables IPv6 egress address filtering.

ipv6 egress-address-filtering
Enables IPv6 egress address filtering.

Usage
Used to filter packets that arrive from the internet to a particular site.

Example
The following command provides an example disabling egress address filtering:
no ipv6 egress-address-filtering
ipv6 initial-router-advt

Creates an IPv6 initial router advertisement interval for the subscriber.

**Product**
PDSN, GGSN, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ipv6 initial-router-advt { interval value | num-advts value }  
default ipv6 initial-router-advt { interval | num-advts }
```

- **default**
  Resets interval or num-advts to their default setting.

- **interval value**
  Default: 3000ms
  The time interval the initial IPv6 router advertisement is sent to the mobile node in milliseconds.
  value is an integer between 100 and 16000 milliseconds.

- **num-advts value**
  Default: 3
  The number of initial IPv6 router advertisements sent to the mobile node.
  value is an integer between 1 to 16.

**Usage**
This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

**Example**
The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```
ipv6 interface-id

Provides an IPv6 interface ID for the subscriber.

Product
PDSN, GGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax
ipv6 interface-id ifid
[ default | no ] ipv6 interface-id

default
No interface id set for IPv6CP negotiation to subscriber.

no
Deletes a previously configured ipv6 interface id.

interface-id ifid
It is a interface ID assigned to the Mobile during IPv6CP negotiation.
ifid is a 64 bit unsigned integer.

Usage
Used to provide a IPv6 ifid for the subscriber when using 6to4 routing.

Example
The following command provides an example of assigning an IPv6 interface ID of 00-00-00-05-47-00-37-44 to the subscriber:
ipv6 interface-id 00-00-00-05-47-00-37-44
ipv6 minimum-link-mtu

Configures the IPv6 minimum-link-MTU value.

Product
PDSN, GGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax

ipv6 minimum-link-mtu value
default ipv6 minimum-link-mtu

default
Resets minimum link MTU to their default setting.
Default: 1280

value
Default: 1280
value is an integer between 100 and 2000 MTUs.

Usage
Used to override the IPv6 minimum link MTU values recommended by the standard.

Example
The following command provides an example of assigning an IPv6 minimum link MTU to 1580 to the subscriber:

ipv6 minimum-link-mtu 1580
ipv6 secondary-address

Configures additional IPv6 4-bit prefixes to the subscriber session.

Product
PDSN, GGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax
[ no ] ipv6 secondary-address { prefix ipv6_address_prefix | prefix-pool pool_name }

no
Deletes a previously configured ipv6 secondary address.

ipv6_address_prefix
The IPv6 secondary address and must be specified using colon notation.

pool_name
The name given to the secondary address prefix pool (a string size from 1 to 31 characters).

Usage
An IPv6 prefix pool name may be configured for a dynamic prefix, while the prefix is static. This command may be executed multiple times to configure multiple prefixes.

Example
The following command provides an example of assigning an IPv6 secondary address prefix-pool name of eastcoast to the subscriber:
ipv6 secondary-address prefix-pool eastcoast
I2tp send accounting-correlation-info

This command enables the L2TP LAC to send accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) in L2TP control message (ICRQ) during session setup to LNS.

**Product**
PDSN, LNS, LAC

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[no | default] i2tp send accounting-correlation-info
```

- **no**
  Disables the command and sets the setting to default mode for this subscriber.

- **default**
  Sets the setting to default mode of disable.

**Usage**

Use this command to enable the L2TP LAC to send accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) in L2TP control message (ICRQ) during session setup to LNS for this subscriber. LNS can be configured to include this information in ECS billing records, so that billing servers can easily correlate accounting records from PDSN/LAC and LNS. By default, this mode is disabled.

**Example**

Following command disables the inclusion of accounting correlation information in control messages during session setup to LNS for a subscriber:

```
default i2tp send accounting-correlation-info
```
13-to-l2-tunnel address-policy

Configure the subscriber address allocation/validation policy, when subscriber L3 (IPV4) sessions are tunneled using an L2 tunneling protocol (e.g. L2TP).

**Product**
HA, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
13-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }
```

default 13-to-l2-tunnel address-policy

- **default**
  Restores the default value for l3-to-l2-tunnel address-policy.

- **alloc-only**
  Only allocate an address in the case of dynamic address assignment. Do not validate static addresses.

- **alloc-validate**
  Locally allocate and validate subscriber addresses.

- **no-alloc-validate**
  Do not allocate or validate subscriber addresses locally in the system for the current subscribers sessions. Pass the address between the remote tunnel terminator and the Mobile Node. This is the default behavior.

**Usage**
Use this command to configure the L3 to L2 tunnel address policy for MIP HA sessions tunneled from the system using L2TP tunnels or for GGSN IP Context sessions tunneled using L2TP to a remote LNS. Also refer to the `resource` keyword of the context configuration mode `ip pool` command.

**Example**
To set the L3 to L2 tunnel address policy so that the current subscriber must have IP addresses allocated and validated locally on the system, enter the following command:

```
13-to-l2-tunnel address-policy alloc-validate
```
loadbalance-tunnel-peers

Configures the load balancing of traffic bound for L2TP tunnels configured on the system for the selected subscriber.

Product
L2TP

Privilege
Security Administrator, Administrator

Syntax
```
loadbalance-tunnel-peers { balanced | prioritized | random }
```

- **balanced**
  Enables the equal use of all configured tunnel peers (LNSs) for the selected subscriber.

- **prioritized**
  Enables the use of all configured tunnel peers (LNSs) for the selected subscriber based on the preference number assigned to the peer address.

- **random**
  Default: Enabled
  Enables the random use of all configured tunnel peers (LNSs) for the selected subscriber.

Usage
Use to manage traffic loads on LAC ports and their respective L2TP Network Servers.

Example
Use the following command to randomly use all configured tunnel peers (LNSs):
```
loadbalance-tunnel-peers random
```
long-duration-action

This command specifies what action is taken when the long duration timer expires.

**Product**

All

**Privilege**

Administrator

**Syntax**

```plaintext
long-duration-action { detection | disconnection [ dormant-only ] [ suppress-notification ] }
```

**detection**

Default: Enabled

Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior. Use this command to detect a session exceeding the limit set by the long duration timer.

**disconnection [ dormant-only ] [ suppress-notification ]**

Default: Disabled

Detects a long duration session and disconnects the session after sending SNMP TRAP and CORBA notification.

**suppress-notification**

Suppress the SNMP TRAP and CORBA notification after detecting and disconnecting a long duration session. Default: Disabled

**dormant-only**

Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. If the long duration timeout is fired and the call is not dormant, the call is disconnected when the call later moves to dormancy.

**Important:** For HA calls, the inactivity-time is considered as gauge for dormancy.

It sends the SNMP TRAP and CORBA notification after disconnecting a long duration session. Default: Disabled

**Usage**

Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.

**Example**

Use the following command to enable disconnecting sessions that exceed the long duration timer:

```plaintext
long-duration-action disconnection
```

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP TRAP and CORBA notification:
long-duration-action disconnection suppress-notification

Use the following command to disconnect the session that is in dormant and exceed the long duration timer and send SNMP TRAP and CORBA notification:

    long-duration-action disconnection dormant-only

Note that in case of HA calls, the inactivity-time is considered as gauge for dormancy.
mobile-ip

Enables/disables the subscriber for mobile IP services and access.

Product
HA, FA

Privilege
Security Administrator, Administrator

Syntax

[no] mobile-ip { allow-aaa-address-assignment | dns-address source-priority { aaa | home-agent } | gratuitous-arp aggressive | home-agent ip_address[alternate] | match-aaa-assigned-address | mn-aaa-removal-indication | mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | mn-ha-shared-keykey | mn-ha-spi spi_num | reverse-tunnel | security-level { ipsec | none } | send { accounting-correlation-info | dns-address | imsi | terminal-verification } }

no
Disables the mobile IP option specified.

allow-aaa-address-assignment
Default: Disabled.
Enables the FA to accept a home address assigned by an AAA server. This should only be configured on the FA side.

dns-address source-priority { aaa | home-agent }
Sets the priority behavior on the FA to use either the DNS IP address information from the HA or the AAA server to include in the the RRP to the MN.
When the no keyword is used in conjunction with the dns-address keyword, information received from both the home-agent and the AAA server is sent if available.
DNS IP address information from the HA comes from the DNS NVSE in the RRP.
DNS IP address information from the AAA server is in the access accept message.
home-agent: If the DNS address is received from the home-agent only that information is sent to the MN. Otherwise the DNS address received from the AAA server is sent.
aaa: If the DNS address is received from the AAA server only that information is sent to MN. Otherwise the DNS address received from the home-agent is sent.
gratuitous-arp aggressive
Default: Disabled.
When enabled, this mode will cause the HA to send out gratuitous ARP messages for all Mobile IP (MIP) registration renewals and handoffs.
To disable this mode, use the no form of this command.

Important: This mode will only work for IP addresses that have been assigned from a static IP address pool.
Subnetwork Configuration Mode Commands

**home-agent ip_address [alternate]**

Specifies the IP address of the mobile IP user’s home agent. *ip_address* must be an IPv4/IPv6 address.

*alternate* - Specifies the secondary, or alternate, Home Agent to use when Proxy Mobile IP HA Failover is enabled.

**match-aaa-assigned-address**

Default: Disabled.

Enables the FA to validate the home address in the RRQ against the one assigned by AAA server. This should only be configured on the FA side.

**mn-aaa-removal-indication**

Default: Disabled.

When enabled, the MN-FA challenge and MN-AAA Authentication extensions are removed when relaying a Registration Request (RRQ) to the Home Agent (HA)

**mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }**

Specifies the encryption algorithm to use.

Default: **hmac-md5**

**hmac-md5**: Use HMAC-MD5 hash algorithm, as defined in RFC-2002bis. This is the default algorithm.

**md5**: Use the MD-5 hash algorithm.

**rfc2002-md5**: Use the MD-5 hash algorithm variant as defined in RFC-2002.

**mn-ha-shared-key key**

This is used to verify the MN-HA Authentication for a local subscriber in the current context. A string or a Hexadecimal number beginning with "0x" up to 127 bytes

**mn-ha-spi spi_num**

Specifies the SPI number. *spi_num* must be an integer from 256 through 4294967295.

**reverse-tunnel**

Default: enabled.

Enables the mobile IP user’s for reverse IP tunnels. The **no** keyword is used to disable this option.

**security-level { ipsec | none }**

Default: none

The security-level option configures the security level needed for the subscriber’s traffic.

**ipsec**: both MIP control and data traffic are secured with IPSEC

**none**: none of the traffic is secured

**Important**: This keyword corresponds to the 3GPP2-Security-Level RADIUS attribute. This attribute indicates the type of security that the home network mandates on the visited network.

**Important**: For this attribute, integer value: 3 : Enables IPSec for tunnels and registration messages 4 : Disables IPSec
send { accounting-correlation-info | dns-address | imsi | terminal-verification }

**accounting-correlation-info**: Configures whether the FA sends the correlation info to the NVSE in the RRQ. Default is disabled.

**dns-address**: Enables the HA to send the DNS address NVSE in the RRP. Default is disabled. This should only be enabled on the HA side.

**imsi**: Configures sending the IMSI NVSE in the RRQ. Default is sending IMSI in custom-1 format.

**terminal-verification**: Enables the FA to send the terminal verification NVSE in the RRQ. Default is disabled. This should only be enabled on the FA side.

**Important**: send dns-address is a proprietary feature developed for a specific purpose and requires the MN to be able to renegotiate IPCP for DNS addresses and reregister MIP if necessary. Since this feature needs the MN to support certain PPP/MIP behavior, and not all MNs may support that particular behavior, send dns-address should be enabled only after careful consideration.

**Usage**

Use as subscriber service contracts change.

**Example**

```
mobile-ip home-agent 1.2.3.4
no mobile-ip reverse-tunnel
```
mobile-ip ha

Accommodates two MIP HA options in subscriber mode.

Product
PDSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

\[
\text{no mobile-ip ha } \{ \text{assignment-table } name \mid \text{ignore-unknown-ha-addr-error} \}
\]

\text{no}
Disables the mobile IP HA option specified.

\text{assignment-table } name
The name of an existing MIP HA Assignment table.
\text{name} must be a string of alphanumeric characters from 1 through 63 characters in length.

\text{ignore-unknown-ha-addr-error}
Default is disabled.
Enables or disables the HA to accept or reject the RRQ from a particular subscriber.

Usage
Use this command to assign a MIP HA Assignment table to the current subscriber.
Use this command to disable or enable the HA to accept or reject the RRQ from a particular subscriber when the HA address in the incoming MIP RRQ is not the same as the HA service address. The feature is off by default which causes the RRQ to be rejected with the error code UNKNOWN_HOME_AGENT.

Example
The following command assigns the MIP HA Assignment table named \text{Atable1} to the current subscriber:
\text{mobile-ip ha assignment-table Atable1}
The following command sets ignore-unknown-ha-addr-error to its default disabled state:
\text{no mobile-ip ha ignore-unknown-ha-addr-error}.
mobile-ip reg-lifetime-override

This command overrides the mobile IP registration lifetime from HA with value configured for subscriber.

**Product**

PDSN, HA, ASN-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
mobile-ip reg-lifetime-override [dur | infinite ]
```

`dur`

Default: 100 secs.
This the configurable value in seconds.
`dur` must be an integer from 1 through 65534.

`infinite`

Sets the mobile IP registration lifetime override value to infinite for a particular subscriber.

`default`

Sets the value of mobile IP registration lifetime override option to 100 seconds.

`no`

Disables the mobile IP registration lifetime override option specified.

**Usage**

Use this command to configure MIP registration-lifetime per realm/domain. This value overrides the default lifetime configured under HA service.

**Example**

The following command overrides the mobile IP registration lifetime value from HA service and assigns the MIP registration lifetime to 100 seconds for the current subscriber:

```
default mobile-ip reg-lifetime-override
```
mobile-ip send accounting-correlation-info

Enables the sending call correlation information NVSE’s to the HA in MIP RRQ.

Product
PDSN, HA, ECS

Privilege
Security Administrator, Administrator

Syntax

[ default | no ] mobile-ip send accounting-correlation-info

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the support for sending call correlation information NCSE’s to the HA in MIP RRQ.</td>
</tr>
<tr>
<td>This is the default mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured support for sending call correlation information.</td>
</tr>
</tbody>
</table>

Usage
Use this command to support PDSN-Correlation-ID VSE and send the call correlation information.

Example
The following command enables sending call correlation information NVSE’s to the HA in MIP RRQ

```bash
mobile-ip send accounting-correlation-info
```
mobile-ipv6

Configures Mobile IPv6 related parameters for a subscriber.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

```
[ default | no ] mobile-ipv6 { home-address ipv6_address / home-agent ipv6_address / home-link-prefix ipv6_address | tunnel mtu value }
```

- **default**
  Disables the support for sending call correlation information NCSE’s to the HA in MIP RRQ. This is the default mode.

- **no**
  Removes the configured support for sending call correlation information.

- **home-address ipv6_address**
  Specifies the home address for the subscriber. `ipv6_address` must be a an IPv6 address in colon notation.

- **home-agent ipv6_address**
  Specifies the IPv6 address of the mobile IP user’s home agent. `ipv6_address` must be a an IPv6 address in colon notation.

- **home-link-prefix ipv6_address**
  Specifies the IPv6 address of the mobile IP user’s home link. `ipv6_address` must be a an IPv6 address in colon notation.

- **tunnel mtu value**
  Configures the tunnel MTU for the IPv6 tunnel between the HA and the mobile node. `value` must be an integer between 1024 and 2000. The default is 1500.

Usage

This command sets the mobile-ipv6 parameters for a subscriber. Use this command to set the home-address, home-agent, and home-link prefix.

Example
Use the following command to set the tunnel value to 1800:

```
mobile-ipv6 tunnel mtu 1800
```
nai-construction-domain

After authentication, the domain name set by this command replaces the NAI constructed domain for subscriber.

Product
All

Privilege
Security Administrator, Administrator

Syntax

nai-construction-domain domain_name
no nai-construction-domain

domain_name
Defines the domain name to use to replace the NAI constructed domain name. This must be a string of 1 to 79 characters.

no
Deletes the defined domain name.

Usage
Define or delete a domain name to use to replace the NAI constructed domain name after authentication.

Example
To set the domain name to private1 use the following command:

nai-construction-domain private1

To delete the previously configured domain name, use the following command:

no nai-construction-domain
**nbns**

Configures and Enables use of NetBios Name Service for the subscriber.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
nbns { primary IPv4-address | secondary IPv4-address }
no nbns { primary [IPv4-address] | secondary [IPv4-address] }
```

**primary**
Designates primary NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

**secondary**
Designates secondary/failover NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

**IPv4-address**
Specifies the IPv4 address used for this service.

**no**
Removes/disables use of a previously configured NetBios Name Service.

**Usage**
This command specifies NBNS parameters. The NBNS option is present for both pdp type IP and pdp type PPP for GGSN.
The system can be configured to use of NetBios Name Service for the APN.

**Example**
The following command configures the subscriber’s NetBios Name Service to primary IP 192.168.1.15:
```
nbns primary 192.168.1.15
```
nexthop-forwarding-address

Configures the next hop forwarding address for the subscriber.

**Product**

PDSN, GGSN, ASN GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
nexthop-forwarding-address ip_address
no nexthop-forwarding-address
```

- **ip_address**
  - Configures the IP address of the nexthop forwarding address.

- **no**
  - Disables this function. This is the default setting.

**Usage**

Use this command to configure the next hop forwarding address for the subscriber.

**Example**

The following command configures the next hop forwarding address to 1.1.1.1 using IPv4:

```
nexthop-forwarding-address 1.1.1.1
```
npu qos

Configures an NPU QoS priority queue for packets from the subscriber.

Product
PDSN, GGSN, ASN GW

Privilege
Security Administrator, Administrator

Syntax
npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }

best-effort
Assigns the best-effort queue priority. This is the lowest priority.

bronze
Assigns the bronze queue priority. This is the third-highest priority.

derive-from-packet-dscp
Default: Enabled
Specifies that the priority is to be determined from the DS field in the packet's TOS octet.

gold
Assigns the gold queue priority. This is the highest priority.

silver
Assigns the silver queue priority. This is the second-highest priority.

Usage
This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.

The system can be configured to determine the priority of a subscriber packet either based on the configuration of the subscriber, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).

Refer to the System Administration and Configuration Guide for additional information on NPU QoS functionality.

Important: This functionality is not supported for use with the PDSN at this time.

Example
The following command configures the subscriber’s priority queue to be gold:

npu qos traffic priority gold
nw-reachability-server

Bind the name of a configured network reachability server to the current subscriber and enable network reachability detection.

Product
HA

Privilege
Security Administrator, Administrator

Syntax
```
nw-reachability server server_name
no nw-reachability server
```

server_name
The name of a network reachability server that has been defined in the current context. This is a string of from 1 through 16 characters.

no nw-reachability server
Delete the name of the network reachability server from the current subscriber's configuration and disable network reachability failure detection for the current subscriber.

Usage
Use this command to define the network reachability server for the current subscriber and enable network reachability failure detection for the current subscriber. If a network reachability server is defined in an IP pool, that setting takes precedence over this command.

Important: Refer to the HA configuration mode command `policy nw-reachability-fail` to configure the action that should be taken when network reachability fails.

Important: Refer to the context configuration mode command `nw-reachability server` to configure network reachability servers.

Important: Refer to the `nw-reachability server server_name` keyword of the `ip pool` command in the context configuration mode chapter to bind the network reachability server to an IP pool.

Example
To bind a network reachability server named `InternetDevice` to the current subscriber, enter the following command:

```
nw-reachability server InternetDevice
```
outbound

Configures the subscriber host password for use in authentication of PPP sessions.

Product  
All

Privilege  
Security Administrator, Administrator

Syntax

```
outbound [encrypted] password pwd
no outbound password
```

```
[ encrypted ] password pwd
```

Specifies the password to use for point-to-point protocol session host authentication. The `encrypted` keyword indicates the password specified uses encryption. The password specified as `pwd` must be from 1 to 63 alpha and/or numeric characters without encryption and must be from 1 to 127 alpha and/or numeric characters when encryption has been indicated. The `encrypted` keyword is intended only for use by the chassis while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

```
no outbound password
```

Used to clear the outbound password configuration from the subscriber data.

Usage

Set the outbound (egress) password for increased security.

Example

```
outbound password secretPwd
outbound encrypted password scrambledPwd
no outbound password
```
overload-disconnect

Sets the threshold parameter for overload disconnect.

Product
ASN GW, HA, PDIF, PDSN, PHS GWPDG/TTG

Privilege
Security Administrator, Administrator

Syntax
overload-disconnect [ threshold { inactivity-time inactivity_time_threshold | connect-time connect_time_threshold } ]

[ default | no ] overload-disconnect [ threshold { inactivity-time | threshold connect-time } ]

threshold inactivity-time inactivity_time_threshold
Sets the inactivity time threshold in seconds. This value must be from 0 to 4294967295. The default value of zero disables this feature. If inactivity-time for the subscriber’s session is greater than inactivity_time_threshold, the session becomes a candidate for disconnection.

threshold connect-time connect_time_threshold
Sets the connection time threshold in seconds. This value must be from 0 to 4294967295. A value of zero disables this feature. If connect-time for the subscriber’s session is greater than connect_time_threshold, the session becomes a candidate for disconnection.

default
This command enables the default condition for this subscriber.

no
Disables the overload disconnect feature for this subscriber. This is the default condition for PDIF.

Usage
Set a subscriber’s overload disconnect threshold in seconds, based on either inactivity or connection time. When this threshold is exceeded during a session, the subscriber’s session becomes a candidate for disconnection. To set overload-disconnect policies for the entire chassis, see congestion-control overload-disconnect in Global Configuration Mode Commands.

Example
overload-disconnect threshold inactivity-time inactivity_time_thresholdDefault
overload disconnect threshold connect-timeno overload-disconnect threshold connect-timeno overload disconnect
password

Configures the subscribers password for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ encrypted ] password p\w d
no password
```

**encrypted**

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

**pwd**

Specifies the users password for authentication. `pwd` must be from 1 to 63 alpha and/or numeric characters or from 1 to 127 characters if the `encrypted` keyword was specified. A “null” password is allowed and is entered as consecutive quotes ("""). See Example(s) for correct syntax.

**Important:** Subscribers configured with a null password will be authenticated using PAP and CHAP (MD5) only. Subscribers configured without a password (`no password`) will only be able to access services if the service is configured to allow no authentication.

**no**

Used to clear the subscriber password configuration from the subscriber data.

**Important:** Subscribers with no password will only be able to access services if the service is configured to allow no authentication.

**Usage**

Password management is critical to system security and all precautions should be taken to ensure passwords are not shared or to easily deciphered.

**Example**

```
password secretPwd password "no password
```
pdif mobile-ip

Configures PDIF subscriber call setup parameters.

Product
PDIF

Privilege
Security Administrator, Administrator

Syntax

[ default | no ] pdif mobile-ip { release-tia | required | simple-ip-fallback }

[ default | no ]
Disables the option specified.

release-tia
Specifies that after subscriber call setup is complete, the tunnel inner address (TIA) is released. If SLimple IP is enabled, the TIA becomes the principal communications tunnel and the restriction that it is only to be used to set up a Mobile-IP call is lifted. This parameter is disabled by default.

required
Specifies that Mobile IP is required for this subscriber whenever a call is set up. This parameter is disabled by default.

simple-ip-fallback
Specifies that Simple IP should be used when Mobile IP could not be established. This parameter is disabled by default.

Usage
Use this command to configure specific behavior for the PDIF subscriber during call setup.

Example
The following command enables the system to fall back to Simple IP when Mobile IP fails for this subscriber during call setup:

    pdif mobile-ip simple-ip-fallback
permission

Enables/disables the ability to access wireless data services for the current subscriber.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

[ no ] permission { ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip }

no
Disables the usage of the specified service.

ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip
ha-mobile-ip: enable/disable the home agent support for mobile IP service.
pdsn-mobile-ip: enable/disable the packet data and foreign agent support for mobile IP service.
pdsn-simple-ip: enable/disable the packet data support for simple IP service.

Usage
This is necessary per the services the subscriber is allowed to access in the current context.

Example

permission pdsn-mobile-ip
no permission ha-mobile-ip
**policy ipv6 tunnel**

Tunnel MTU for IPv6 Tunnel between HA and Mobile Node.

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
policy ipv6 tunnel mtu exceed { fragment | notify-sender }
```

- `mtu exceed {fragment | notify-sender}`
  - `fragment`: Adjust Tunnel MTU and Fragment Packets
  - `notify-sender`: Send a ICMPv6 Packet Too Big the original sender

**Usage**

Use this command to configure Tunnel MTU for IPv6 Tunnel between HA and Mobile Node.

**Example**

```plaintext
policy ipv6 tunnel mtu exceed fragment
```
policy-group

This command assigns/removes a flow-based traffic policy group to a subscriber.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] policy-group policy_group_name direction { in | out }
```

- **no**
  - Removes assigned policy group from a subscriber configuration.

- **policy_group_name**
  - Specifies the traffic policy group name for a subscriber session flow pre-configured within a destination context.
  - `policy_group_name` consist of from 1 to 15 alpha and/or numeric characters in length and is case sensitive.

- **direction { in | out }**
  - Specifies the direction of flow in which the traffic policies need to be applied.
    - `in`: specifies the incoming traffic
    - `out`: specifies the outgoing traffic

**Usage**

Use this command to assign traffic policy group to a subscriber for traffic policing.

**Example**

```
policy-group traffic_policy_group1 direction in
```
ppp

Configures the point-to-point protocol options for the current subscriber.

**Product**

PDSN, GGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ppp { accept-peer-ipv6-ffid | always-on-vse-packet | data-compression { mode { normal | stateless } | protocols { protocols[protocols] } | ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } } } | ipv4 { disable | enable | passive } | ipv6 { disable | enable | passive } | keepalive seconds | min-compression-size min_octets | mtu max_octets | remote-renegotiation disconnect { always | nai-prefix-msid-mismatch } }
```

```
default ppp { accept-peer-ipv6-ffid | always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation { vj compress-slot-id } | ipv4 | ipv6 | keepalive | min-compression-size | mtu | remote-renegotiation disconnect }
```

```
no ppp { accept-peer-ipv6-ffid | always-on-vse-packet | data-compression protocols | ipv4 | ipv6 | keepalive | mtu | remote-renegotiation disconnect }
```

---

**default**

Restores the default value for the option specified.

**no**

Resets the option specified to its default.

### always-on-vse-packet

Default: Enabled

If the always-on feature is enabled for a session, this keyword enables the PDSN to send special 3GPP2 VSE PPP packets to the Mobile Node with a max inactivity timer value. This configuration is applicable only for PDSN sessions.

### accept-ipv6-peer-ffid

Default: None

This is used to configure a 6to4 tunnel. It controls the behavior of IPv6CP negotiation for Interface ID. If enabled, PDSN will accept a valid interface-id proposed by the peer.

### data-compression { mode { normal | stateless } | protocols { protocols [ protocols ] } }

Default: all protocols enabled.

Specifies the subscriber’s mode of data compression or the compression protocol to use.

**mode**: sets the mode of compression where *modes* must be one of:
Subscriber Configuration Mode Commands

- normal (packets are compressed using the packet history for automatic adjustment for best compression)
- stateless (each packet compressed individually)

protocols: sets the compression protocol where protocols must be one of:
- deflate (DEFLATE algorithm)
- mppc (Microsoft PPP algorithm)
- stac (STAC algorithm)

ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } }

Default: force

PPP IP compression Van Jacobson (VJ) negotiation scheme. This command is applicable only if IP header compression is enabled for the subscriber.

detect: The local side does not include the VJ Compression option in its IPCP configuration request unless the peer sends an IPCP NAK including a VJ compression option. If the peer requests the VJ compression option in its IPCP request the local side will ACK/NAK.

force: The IP header compression negotiation in IPCP happens normally. The local side requests the VJ compression option in its IPCP configure request. If the peer side requests VJ compression in its IPCP request, the local side will ACK/NAK the option.

vj compress-slot-id { both | none | receive | transmit }:

- both: If the client proposes VJ slotid compression, accept it and propose slotid compression for downlink and uplink.
- none: If the client proposes VJ slotid compression, NAK the offer, do not propose slotid compression for downlink.
- receive: (Default) If the client proposes VJ slotid compression in the uplink direction accept the configuration.
- transmit: Propose VJ slotid compression for uplink.

ipv4 { disable | enable | passive }

Default: enable

Controls IPCP negotiation during PPP negotiation.

disable: The PDSN does not negotiate IPCP with the mobile.

enable: The PDSN negotiates IPCP with the mobile.

passive: The PDSN initiates IPCP only when the mobile sends an IPCP request.

ipv6 { disable | enable | passive }

Default: enable

Controls IPv6CP negotiation during PPP negotiation.

disable: The PDSN does not negotiate IPCP with the mobile.

enable: The PDSN negotiates IPCP with the mobile.

passive: The PDSN initiates IPCP only when the mobile sends an IPCP request.

keepalive seconds

Default: 30

Specifies the frequency of sending the Link Control Protocol keep alive messages. seconds must be either 0 or in the range from 5 to 14400.
The special value 0 disables the keep alive messages entirely.

**min-compression-size** `min_octets`
Default: 128
Specifies the smallest packet to which compression may be applied. `min_octets` must be a value in the range from 0 to 2000.

**mtu** `max_octets`
Default: 1500
Specifies the maximum size in octets the message transfer unit packets can reach. `max_octets` must be a value in the range from 100 to 2000.

**remote-renegotiation disconnect** `{ always | nai-prefix-msid-mismatch }`
Default: Disabled
Terminates the already established PPP sessions if they are renegotiated by the remote side by sending LCP Conf-req/nak/ack. The following termination conditions are available:

- **always**: The session is automatically disconnected.
- **nai-prefix-msid-mismatch**: The session is disconnected only if the MSID of the session does not match NAI-Prefix (prefix before “@” for the NAI). The configuration of the renegotiated (new) NAI is used for the matching process.

**Usage**
Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

**Example**

```
ppp data-compression protocols mode statelesppp mtu 500no ppp data-compression protocolsno ppp keepalive
```
prepaid 3gpp2

Enables 3GPP2 compliant prepaid billing support for a subscriber to be configured by 3GPP2 attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored.

Product
HA, PDSN

Privilege
Security Administrator, Administrator

Syntax

```
prepaid3gpp2 { accounting [ no-final-access-request ] | duration-quota final-duration-algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time } | preference { duration | volume } }
```

```
default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }
```

```
no prepaid3gpp2accounting
```

```
default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }
```

Sets the 3GPP2 Pre-paid settings to the default values.

- **duration-quota final-duration-algorithm:** Reset the end of billing duration quota algorithm to the default of current-time.
- **preference:** Reset the preference to duration, If both duration and volume attributes are present.

```
no prepaid 3gpp2 accounting
```

Disables 3GPP2 prepaid accounting. All 3GPP2 Prepaid attributes received from a RADIUS server are ignored.

```
accounting [ no-final-access-request ]
```

Default: Disabled
Enabled 3GPP2 prepaid accounting behavior.

Sets the low-watermark for remaining byte credits. `percentage` is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. `percentage` must be an integer from 1 to 99.

```
no-final-access-request
```

Disables 3GPP2 prepaid accounting. By default, this option is disabled.

```
duration-quota final-duration-algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time }
```

Define what behavior specifies the end of the billing duration for duration-based quota usage accounting. The default behavior is the duration quota algorithm set to current-time.
Default: current-time

```
current-time
```

Selects the duration quota as the difference between the session termination timestamp and the session setup timestamp.

```
last-airlink-activity-time
```

Selects the duration quota as the difference between the last-user-activity timestamp (G17) and the session setup timestamp.
last-user-layer3-activity-time: Selects the duration quota as the difference between the timestamp of the last layer-3 packet sent to or received from the user and the session setup timestamp.

preference { duration | volume }
If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.
Default: duration
duration: The duration attribute takes precedence.
volume: The volume attribute takes precedence

Usage
Use this command to enable prepaid support for a default user or for the default user of a domain alias.

Example
The following command enables 3GPP2 prepaid support for the default user:
prepaid 3gpp2 accounting
prepaid custom

Enables custom prepaid billing support for a subscriber to be configured by attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored. The keywords are to set prepaid values that are used if the corresponding RADIUS attribute is not present. If the RADIUS attribute is present it takes precedence over these values.

Product
HA, PDSN

Privilege
Security Administrator, Administrator

Syntax

```plaintext
prepaidcustom { accounting | byte-count compressed | low-
watermarkpercentage | renewalintervalseconds } | preference { duration |
volume }

defaultprepaidcustom { byte-count | low-watermark }

noprepaidcustom { accounting | byte-count compressed | low-watermark | renewal }
```

```plaintext
default prepaid custom { byte-count | low-watermark }

Resets custom prepaid settings to the default values.

byte-count: Reset to the default of basing the prepaid byte credits on the flow of uncompressed traffic.

low-watermark: Disable sending an access request to retrieve more credits when a low watermark is reached.
```

```plaintext
no prepaid custom { accounting | byte-count compressed | low-watermark | renewal}
```

byte-count compressed: The prepaid byte credits are based on the flow of uncompressed traffic. This is the default.

low-watermark: Disables the low watermark feature. An access-request isn’t sent to the RADIUS server until the credits granted for the subscriber session are depleted.

renewal: Disables time-based renewals for prepaid accounting.

accounting

Default: Disabled
Enabled custom prepaid accounting behavior.

byte-count compressed

Default: uncompressed.
When compression is used, the prepaid byte credits are based on the flow of compressed traffic. The default is to base the prepaid byte credits on the flow of uncompressed traffic.

low-watermark percent percentage

Default: Disabled.
Sets the low-watermark for remaining byte credits. *percentage* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *percentage* must be an integer from 1 to 99.

**renewal interval seconds**

Default: The time in seconds to wait before sending a new RADIUS access-request to the RADIUS server to retrieve more credits. *seconds* must be an integer from 60 through 65535.

**preference { duration | volume }**

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.

Default: duration

**duration:** The duration attribute takes precedence.

**volume:** The volume attribute takes precedence

**Usage**

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

**Example**

The following command enables custom prepaid support for the default user:

```
prepaid custom accounting
```
prepaid unclassify

This command provides customer specific functionality.
prepaid voice-push

This command provides customer specific functionality.
**prepaid wimax**

Enables WiMAX prepaid accounting for this subscriber. This feature is disabled by default.

**Product**
ASN GW

**Privilege**
Administrator

**Syntax**

```
[ no ] prepaid wimax accounting
```

- **no**
  
  Disables WiMAX prepaid accounting for this subscriber.

**Usage**

Use this command to enable WiMAX prepaid accounting for this subscriber.
proxy-dns intercept list-name

Identifies a proxy DNS intercept rules list for the selected subscriber.

Product
HA

Privilege
Security Administrator, Administrator

Syntax

[ no ] proxy-dns intercept list-name name

no
Remove the intercept list from the subscriber’s profile.

proxy-dns intercept list-name name
Specifies a name of a proxy DNS intercept list used for the selected subscriber.
name is the name of the intercept list and must be a string from 1 to 63 characters in length.

Usage
Use this command to identify a proxy DNS rules list for the selected subscriber. For a more detailed explanation of the HA Proxy DNS Intercept feature, see the proxy-dns intercept-list command in the Context Configuration Mode Commands chapter.
proxy-mip

Configures support for Proxy Mobile IP for the subscriber.

Product
PDSN, GGSN, ASN GW, PDIF

Privilege
Security Administrator, Administrator

Syntax

[ no ] proxy-mip required

no
Disables support for Proxy Mobile IP.

required
Enables support for Proxy Mobile IP.

Usage
When enabled through the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP. For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established as they would for a Simple IP session. However, the AGW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber’s profile) on behalf of the MN while the MN performs only Simple IP processes.

Example
The following command enables proxy mobile IP for the current subscriber:

proxy-mip required
qos rate-limit

Configure the action on subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality. When configured, the PDG/TTG performs traffic policing for the subscriber session. If the GGSN changes the QoS via an Update PDP Context Request, the PDG/TTG uses the new QoS values for traffic policing.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Syntax
```
qos rate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ]
[ exceed-action { drop | lower-ip-precedence | transmit } ][ violate-action { drop | lower-ip-precedence | transmit } ]
noqosrate-limitdirection{ downlink | uplink } { class { background | conversational | interactive traffic_priority | streaming } }
```

no
Disables the QoS data rate limit configuration for the APN.

downlink
Apply the specified limits and actions to the downlink (to the data coming from the GGSN over the Gn’ interface).

uplink
Apply the specified limits and actions to the uplink (to the data coming from the UE over the IPSec tunnel).

class { background | conversational | interactive traffic_priority | streaming }
Apply the specified limits and actions to the PDP contexts of the specified UMTS traffic class. The following classes are supported:

- **background**: Specifies the QoS for traffic patterns in which the data transfer is not time-critical (for example, e-mail exchanges). This traffic pattern should be the lowest QoS.

- **conversational**: Specifies the QoS for traffic patterns in which there is a constant flow of packets in each direction, upstream and downstream. This traffic pattern should be the highest QoS.

- **interactive traffic_priority**: Specifies the QoS for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. This traffic pattern should be a higher QoS than the background pattern, but not as high as that for the streaming pattern. The traffic_priorityis the 3GPP traffic handling priority and can be the integers 1, 2, or 3.

- **streaming**: Specifies the QoS for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream. This traffic pattern should be a higher QoS than the interactive pattern, but not as high as that for the conversational pattern.
Important: If this keyword is omitted, the same values are used for all classes.

```
exceed-action { drop | lower-ip-precedence | transmit }
```

Default: See Usage section for this command

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate.

The following actions are supported:

- **drop**: Drop the packet.
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence.
- **transmit**: Transmit the packet.

```
vio late-action { drop | lower-ip-precedence | transmit }
```

Default: See Usage section for this command

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet.
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence.
- **transmit**: Transmit the packet.

**Usage**

This command configures the APN’s quality of service (QoS) data rate shaping through traffic policing. This command enables the actions on subscriber flow exceeding or violating peak/committed data rate allowed. The shaping function also provides an enhanced function to buffer the exceeded user packets in a buffer memory and sends them to the subscriber when subscriber traffic goes below the committed or peak data rate limit.

Important: The user packet buffer function in traffic shaping is not applicable for real-time traffic.

Important: If the exceed/violate action is set to “lower-ip-precedence”, this command may override the configuration of the `ip qos-dscp` command in the GGSN service configuration mode for packets from the GGSN to the PDG/TTG. In addition, the GGSN service `ip qos-dscp` command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the PDG/TTG (i.e., it accepts all of the PDG/TTG-provided values for the PDP context.

Important: This command should be used in conjunction with the max-contexts command to limit the maximum possible bandwidth consumption by the APN.

Additional information on the QoS traffic shaping and policing functionality is located in the *System Enhanced Feature Configuration Guide*.

Default values:

The following table displays the default values for each of the traffic classes:
<table>
<thead>
<tr>
<th>Class: Conversational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Streaming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Background</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 1600000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Example**
The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```
**qos traffic-policing**

Enables and configures traffic policing through the bandwidth limits and action for the subscriber traffic if it exceeds/violates the peak or committed data rate. Uplink and downlink limits are configured separately.

**Product**
PDSN, HA, GGSN, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
qos traffic-policing {downlink|uplink} [burst-size bytes] [committed-data-rate bps] [exceed-action {drop|lower-ip-precedence|transmit}] [peak-data-rate bps] [violate-action {drop|lower-ip-precedence|transmit}]
```

```
no qos traffic-policing {downlink|uplink}
```

**downlink**

Apply the specified limits and actions to the downlink (data to the subscriber).

**uplink**

Apply the specified limits and actions to the uplink (data from the subscriber).

**burst-size bytes**

Default: 3000
The peak burst size allowed, in bytes.

*important*: It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

**committed-data-rate bps**

Default: 144000
The committed data rate (guaranteed-data-rate) in bps (bits per second).

*important*: It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

**exceed-action { drop | lower-ip-precedence | transmit }**

Default: lower-ip-precedence
The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate.

The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence
- **transmit**: Transmit the packet
peak-data-rate \textit{bps}

Default: 256000
Specifies the peak data-rate for the subscriber, in bps (bits per second).
\textit{bps} must be an integer from 0 through 4294967295.

\textbf{violate-action} \{ \textit{drop} | \textit{lower-ip-precedence} | \textit{transmit} \}

Default: \textit{drop}
The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
\textit{drop}: Drop the packet
\textit{lower-ip-precedence}: Transmit the packet after lowering the IP precedence
\textit{transmit}: Transmit the packet

\textbf{no}
Disable traffic policing for the specified direction for the current subscriber.

\textbf{Usage}
Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions.

\begin{itemize}
    \item \textbf{Important:} If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the \texttt{ip user-datagram-tos copy} command is configured to. In addition, the “lower-ip-precedence” option may also override the configuration of the \texttt{ip qos-dscp} command. Therefore, it is recommended that command not be used when specifying this option.
\end{itemize}

Details on the QoS traffic policing functionality is located in the System Enhanced Feature Configuration Guide.

\textbf{Example}
The following command sets an uplink peak data rate of 128000 bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:
\texttt{qos traffic-policy direction uplink peak-data-rate 128000 violate-action lower-ip-precedence}
The following command sets a downlink peak data rate of 256000 bps and drops packets when the committed-data-rate and the peak-data-rate are exceeded:
\texttt{qos traffic-policy direction downlink peak-data-rate 256000 violate-action drop}
**qos traffic-shape**

Enables and configures traffic shaping functionality to provide the traffic shaping by means of buffering the data packets during congestion or when subscriber exceeds the configured peak or committed data rate limit. It buffers the data packets instead of discarding instantaneous burst and deliver it to subscriber when traffic flow is below the peak or committed data rate. Uplink and downlink traffic shaping are configured separately.

---

**Important:** This feature is NOT supported for real-time traffic.

**Product:**

PDSN, HA, GGSN, ASN GW

**Privilege:**

Security Administrator, Administrator

**Syntax**

```
qos traffic-shape direction { downlink | uplink } [ burst-size bytes ] [ committed-data-rate bps ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ peak-data-rate bps ] [ violate-action { drop | lower-ip-precedence | transmit } ] +
no qos traffic-shape direction { downlink | uplink }
```

**downlink**

Apply the specified limits and actions to the downlink (data to the subscriber).

**uplink**

Apply the specified limits and actions to the uplink (data from the subscriber).

**burst-size bytes**

Default: 3000

The peak burst size allowed, in bytes.

*bytes* must be an integer from 0 through 4294967295.

---

**Important:** It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

**committed-data-rate bps**

Default: 144000

The committed data rate (guaranteed-data-rate) in bps (bits per second).

*bps* must be an integer from 0 through 4294967295.

**exceed-action { drop | lower-ip-precedence | transmit }**

Default: lower-ip-precedence
The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate.
The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence
- **transmit**: Transmit the packet

---

### peak-data-rate bps

Default: 256000

Specifies the peak data-rate for the subscriber, in bps (bits per second).

- **bps** must be an integer from 0 through 4294967295.

---

### violate-action { drop | lower-ip-precedence | buffer [transmit-when-buffer-full] | transmit }

Default: See Usage section for this command

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence
- **buffer [transmit-when-buffer-full]**: Enables the traffic shaping and provides the buffering of user packets when subscriber traffic violates the allowed peak/committed data rate. The **[transmit-when-buffer-full]** keyword allows the packet to be transmitted when buffer memory is full.
- **transmit**: Transmit the packet

---

+ More than one of the above keywords can be entered within a single command.

---

### no

Disable traffic policing for the specified direction for the current subscriber.

---

### Usage

Use this command to provide the traffic shaping function to a subscriber in the uplink and downlink directions. This feature is providing a traffic flow control different to QoS traffic policing. When a subscriber violates or exceeds the peak data rate instead of dropping the packets, as in QoS traffic policing, this feature provides the buffering facility of subscriber data packets and it sends the buffered data when the traffic flow is low or not in congestion state.

---

**Important:** If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the **ip user-dgram-tos copy** command is configured to. In addition, the “lower-ip-precedence” option may also override the configuration of the **ip qos-dscp** command. Therefore, it is recommended that command not be used when specifying this option.

---

Details on the QoS traffic policing functionality is located in the System Enhanced Feature Configuration Guide.

---

### Example
The following command sets an uplink peak data rate of 128000 bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-shape direction uplink peak-data-rate 128000 violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak-data-rate 256000 bps in downlink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos traffic-shape direction downlink peak-data-rate 256000 violate-action buffer transmit-when-buffer-full
```
radius accounting

Sets the RADIUS accounting parameters for the subscriber or domain. This command takes precedence over the similar context configuration command. This command is disabled by default.

Product
All

Privilege
Administrator

Syntax

radius accounting { interim { interval-timeout timeout } | ip remote-address list-id list_id | mode { session-based | access-flow-based { none | auxiliary-flows | all-flows | main-a10-only } } | start { normal | suppress } | stop { normal | suppress } }

no radius accounting { ip remote-address list-id list_id | interim { interval-timeout } }

| interim { interval-timeout timeout | normal | suppress } |
| interval-timeout timeout: Indicates the time (in seconds) between updates to session counters (log file on RADIUS or AAA event log) during the session. timeout must be an integer from 50 to 4000000.

Caution: Interim interval settings received from the RADIUS server take precedence over this setting on the system. While the low limit of this setting on the system is a minimum of 50 seconds, the low limit setting on the RADIUS server can be as little as 1 second. To avoid increasing network traffic unnecessarily and potentially reducing network and system performance, do not set this parameter to a value less than 50 on the RADIUS server.

| normal: If RADIUS accounting is enabled, send this Acct-Status-Type message when required by normal operation |
| suppress: If RADIUS accounting is enabled, suppress the sending of this Acct-Status-Type message. |

ip remote-address list-id list_id

Specifies the identification number of the IP address list to use for the subscriber for remote address-based accounting.

list_id: Specify the RADIUS accounting remote IP address list identifier for remote-address accounting for the subscriber. list_id must be an integer from 1 through 65535.

This command is used as part of the Remote Address-based accounting feature and associates the subscriber with a list of remote addresses. Remote address accounting data is collected each time the subscriber communicates with any of the addresses specified in the list.

Remote address lists are configured using the list keyword in the radius accounting ip remote-address command in the Context Configuration mode.

mode { session-based | access-flow-based { none | auxiliary-flows | all-flows | main-a10-only } }

Default: session-based

Specifies if the radius accounting mode is either session-based or access-flow-based.
**session-based**: configures session-based RADIUS accounting behavior for the subscriber - which means a single radius accounting message generated for the subscriber session not separate accounting messages for individual A10 connections or flows.

**access-flow-based**: configures access-flow-based RADIUS accounting behavior for the subscriber. This offers flexibility by generating separate accounting messages for flows and A10 sessions.

- **all-flows**: Generates separate RADIUS accounting messages per access flow. Separate accounting messages are not generated for data path connections. (For example, separate messages are not sent for the main A10 or auxiliary connections.).

- **auxiliary-flows**: Generates RADIUS accounting records for the main data path connection and for access-flows for all auxiliary data connections. (For example, separate RADIUS accounting messages are generated for the main A10 session and for access-flows within auxiliary A10 connections. The main A10 session accounting does not include octets or other accounting information from the auxiliary flows.)

- **main-a10-only**: Configures access-flow-based single accounting messages (for example only single start/interim/stop) are generated for the main A-10 flows only.

- **none**: Separate RADIUS accounting messages are generated for all data path connections (for example, PDSN main or auxiliary A10 connections) but not for individual access-flows. This is essentially A10 connection-based accounting.

```
start { normal | suppress }
```

**normal**: If RADIUS accounting is enabled, send this Acct-Status-Type message when required by normal operation

**suppress**: If RADIUS accounting is enabled, suppress the sending of this Acct-Status-Type message.

```
stop { normal | suppress }
```

**normal**: If RADIUS accounting is enabled, send this Acct-Status-Type message when required by normal operation

**suppress**: If RADIUS accounting is enabled, suppress the sending of this Acct-Status-Type message.

```
o
```

**no**

Sets the accounting message start normal for main A-10 flows only.

### Usage

Use this command to allow a per-domain setting for the RADIUS accounting.

### Example

Set the accounting interim interval to one minute (60 seconds) for all sessions that use the current subscriber configuration:

```
radius accounting interim interval-timeout 60
```

Do not send RADIUS interim accounting messages:

```
radius accounting interim suppress
```

Sets the accounting message start normal for main A-10 flows only.
radius accounting mode main-a10-only start normal
radius group

It applies a RADIUS server group at the subscriber level for AAA functionality.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
radius group group_name
```

**group_name**

Specifies the name of the server group that is used for authentication and/or accounting for the specific subscriber.

*group_name* must be a string of size 1 to 63 characters. It must be the same as configured earlier within the same context of subscriber.

```bash
default
```

Sets / Restores default RADIUS server group specified at the context level or default subscriber profile.

```bash
no
```

Disables the applied RADIUS group for specific subscriber.

**Usage**

This feature provides the RADIUS configurables under radius group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual RADIUS server group for a subscriber in that context. Each server group consists of a list of AAA servers. In case no RADIUS group is applied for the said subscriber or default subscriber profile, then the default server group available at context level is applicable for accounting and authentication of specific subscriber.

**Example**

Following command applies a previously configured RADIUS server group named *star1* to a subscriber within the specific context:

```bash
radius group star1
```

Following command disables the applied RADIUS server group for the specific subscriber.

```bash
no radius group
```
radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Product
GGSN

Privilege
Security Administrator, Administrator

Syntax

radius returned-framed-ip-address 255.255.255.255-policy {accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied}

default radius returned-framed-ip-address 255.255.255.255-policy

accept-call-when-ms-ip-not-supplied
Accept calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.

reject-call-when-ms-ip-not-supplied
Reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.

default
Set the policy to its default of rejecting calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.

Usage
Use this command to set the behavior for the current subscriber when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Example
Use the following command to set the subscriber profile to reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address:

radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied
**rohc-profile-name**

Identifies the RoHC profile configuration to be applied to bearer sessions belonging to this subscriber.

**Product**

HSGW,PDSN

**Privilege**

Administrator

**Syntax**

```
rohc-profile-name name
```

`name`

Specifies the name of the RoHC profile this subscriber will use to apply header compression and decompression parameters to bearer session data. `name` must be an existing RoHC profile and be from 1 to 63 alpha and/or numeric characters.

**Usage**

Use this command to specify a RoHC configuration profile to be applied to bearer sessions belonging to this subscriber. RoHC profiles are configured through the Global Configuration Mode using the `rohc-profile` command.

**Example**

The following command specifies that the RoHC profile named `rohc-cfg1` is to be applied to all bearer sessions belonging to this subscriber:

```
rohc-profile-name rohc-cfg1
```
secondary ip pool

This command specifies a secondary IP pool to be used as backup pool for NAT.

Important: This command is license dependent, requiring the 600-00-7871 NAT Bypass license. Please contact your local sales representative for more information.

Product
NAT

Privilege
Security Administrator, Administrator

Syntax

```
secondary ip pool pool_name
no secondary ip pool
```

no
Removes the previous secondary IP pool configuration.

```
pool_name
```
Specifies the secondary IP pool name.
`pool_name` must be an alpha and/or numeric string of 1 through 31 characters in length.

Usage
Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool configured will be appended to the RADIUS supplied IP pool list / subscriber template provided IP pool list whichever is applicable during call setup.

Example
The following command configures a secondary IP pool named `test123`:

```
secondary ip pool test123
```
simultaneous

Enables/disables the simultaneous use of both Mobile and Simple IP services.

Product
PDSN, FA, HA, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

```plaintext
[ no ] simultaneous simple-and-mobile-ip
```

```plaintext
no
```

Disables the simultaneous use.

Usage
Subscribers with mobile devices supporting mobile and simple IP services concurrently require this option to be set.

Example

```plaintext
no simultaneous simple-and-mobile-ip
simultaneous simple-and-mobile-ip
```
timeout

Configures the subscriber session timeouts.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
timeout { absolute | idle } seconds
no timeout [ absolute | idle ]
```

**absolute**
Default: 0
The absolute maximum time a session may exist in any state (active or dormant).

**idle**
Default: 0
The maximum duration of the session, in seconds, before the system automatically terminates the session due to inactivity.

**seconds**
Specifies the maximum amount of time, in seconds, before the specified timeout action is activated. **seconds** must be a value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

**no**
Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

Usage

Reduce the idle timeout to free session resources faster for use by new requests.

Example

```
timeout absolute 1800
no timeout
```
timeout idle-time

This command configures the idle timeout configuration timer for subscriber session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
timeout idle-time idle_timeout
no timeout idle-time
```

- **idle_timeout**
  
  Default: 0
  
  Designates the maximum duration of the session, in seconds, after the expiry of which the system disconnects the subscriber.
  
  *idle_timeout* must be a value in the range from 0 through 4294967295.
  
  The special value 0 disables the timeout specified.

- **no**
  
  Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

**Usage**

Use this command to set the idle time after which the call has to be disconnected.

**Example**

Following command sets the idle timeout duration to 450 seconds.

```
timeout idle-timeout 450
```
timeout long-duration

Configures the long duration timeout and optionally the inactivity duration of HA subscriber session.

Product
All

Privilege
Security Administrator, Administrator

Syntax

timeout-long-duration ldt_timeout [ inactivity-time inact_timeout]

[ no | default ]timeoutlong-duration

no
Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

long-duration ldt_timeout
Default: 0
Designates the maximum duration of the session, in seconds, before the system automatically reports/terminates the session.
ldt_timeout must be a value in the range from 0 through 4294967295.
The special value 0 disables the timer.

inactivity-time inact_timeout
Specifies the maximum amount of time, in seconds, before the specified session is marked as dormant.
inact_timeout must be a value in the range from 0 through 4294967295.
The special value 0 disables the inactivity time specified.

Usage
Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests. Refer to the long-duration-action detection and long-duration-action disconnection section for more information.

Example
Following command sets the long duration timeout duration to 300 seconds and inactivity timer for subscriber session to 45 seconds.
timeout long-duration 300 inactivity-time 45
tunnel address-policy

This command specifies the policy for address allocation and validation for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. This means that GGSN IP address validation could be disabled for specified incoming calls.

For GGSN systems, this command can also be specified in the APN Configuration mode (tunnel address-policy) which would mean the system defers to the old 13-to-12-tunnel address policy command for calls coming through L2TP tunnels.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default tunnel address-policy

---

alloc-only
IP addresses are allocated locally and no validation is done.

alloc-validate
Default.
The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

no-alloc-validate
No IP address assignment or validation is done for calls coming in via L3 tunnels. Incoming static IP addresses are passed. This allows for the greatest flexibility.

default
Resets the tunnel address-policy to alloc-validate.

---

Usage
This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignment. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.

Example
Use the following command to reset the IP address validation policy to validate against a static pool of address:

default tunnel address-policy

Use the following command to disable all IP address validation for calls coming through tunnels:

tunnel address-policy no-alloc-validate
Subscriber Configuration Mode Commands

Cisco ASR 5000 Series Command Line Interface Reference
tunnel gre

Configures Generic Routing Encapsulation (GRE) tunnel parameters for the current subscriber.

Product
PDSN, GGSN, ASN-GW

Privilege
Security Administrator, Administrator

Syntax

**tunnel gre peer-address peer_address**
**local-address local_addr**

**no tunnel gre peer-address peer_address**

**peer-address peer_address**
Specifies the IP address of the external gateway terminating the GRE tunnel.

**local-address local_addr**
Specifies the IP address of the interface in the destination context originating the GRE tunnel.

**no**
Disables GRE tunneling for the current subscriber.

Usage
Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the AGW to an external gateway.

Example
The following command configures the system to encapsulate subscriber traffic using GRE and tunnel it from a local address of 192.168.1.100 to a gateway with an IP address of 192.168.1.225:

```
tunnel gre peer-address 192.168.1.225 local-address 192.168.1.100
```
tunnel ipip

Configures IP-in-IP tunnelling parameters for the current subscriber.

Product
PDSN, GGSN

Privilege
Security Administrator, Administrator

Syntax

```
tunnel ipip peer-address peer_address local-address local_addr
no tunnel ipip
```

**peer-address peer_address**
Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.

**local-address local_addr**
Specifies the IP address of the interface in the destination context originating the IP-in-IP tunnel.

**no**
Disables IP-in-IP tunneling for the current subscriber.

**Usage**
Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN or PDSN to an external gateway.

**Example**
The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of 192.168.1.100 to a gateway with an IP address of 192.168.1.225:

```
tunnel ipip peer-address 192.168.1.225
local-address 192.168.1.100
```
tunnel ipsec

This command configures sessions for the current subscriber to use an IPSEC tunnel based on the IP pool corresponding to the subscribers assigned ip address.

**Product**
PDSN, GGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
tunnel ipsec use-policy-matching-ip-pooler-address
no tunnel ipsec [ use-policy-matching-ip-pooler-address ]
```

- **no**
  Disables the use of the IPSEC policy that matches the IP pool that the assigned IP address relates to.

**Usage**

Use this command to set the current subscribers sessions to use an IPSEC policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

**Example**
The following command enables the use of the policy that matches the IP pool address:
```
tunnel ipsec use-policy-matching-ip-pooler-address
```
tunnel l2tp

Configures the L2TP tunnel for the subscriber.

Product
L2TP

Privilege
Security Administrator, Administrator

Syntax

```
tunnel l2tp [ peer-address ip_address [ [ encrypted ] [ secret secret ] ] [ preference number ] [ tunnel-context context ] [ local-address ip_address ] [ crypto-map map_name [ [ encrypted ] isakmp-secret secret ] ] ]
```

```
no tunnel l2tp [ peer-address ip_address ]
```

**peer-address ip_address**

A peer L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). ip_address must be an IP address in IPv4/IPv6 format.

```
[ [ encrypted ] secret secret ]
```

The shared key (secret) between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). secret must be between 1 and 63 alpha and/or numeric characters and is case sensitive. **encrypted**: The encrypted shared key between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). secret must be between 1 and 128 alpha and/or numeric characters and is case sensitive. The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

**preference number**

Default: 1

The order in which a group of tunnels configured for this subscriber will be tried. number must be an integer between 1 and 65535.

**tunnel-context context**

The name of the context containing ports through which this subscriber’s data traffic is to be communicated between this LAC and the LNS. context must be between 1 and 79 alpha and/or numeric characters.

**local-address ip_address**

A LAC service bind address which is given as a hint used to select a particular LAC service. ip_address must be an IP address in IPv4/IPv6 format.
crypto-map map_name { [encrypted] isakmp-secret secret }

map_name is the name of a crypto map that has been configured in the current context. map_name must be a string from 1 to 127 alphanumeric characters.

isakmp-secret secret: The pre-shared key for IKE. secret must be a string from 1 to 127 alphanumeric characters.

encrypted isakmp-secret secret: The pre-shared key for IKE. Encryption must be used when sending the key. secret must be a string from 1 to 127 alphanumeric characters.

no

Disables tunneling for the current subscriber. When peer-address is included, the tunneling for that specific L2TP Network Server (LNS) is disabled but tunneling to other configured LNSs is still enabled.

Usage

Use this command to configure specific L2TP tunneling parameters for the current subscriber.

Example

To specify L2tp tunneling to the LNS peer at the IP address 198.162.10.100 with a shared secret of bigco and preference of 1, enter the following command:

tunnel l2tp peer-address 198.162.10.100 secret bigco preference 1
Chapter 197
Telnet Configuration Mode Commands

The Telnet Configuration Mode is used to manage the Telnet server options for the current context.
end

Exits the telnet server configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the telnet server configuration mode and returns to the context configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
**max servers**

Configures the maximum number of telnet servers that can be started within any 60 second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
max servers count
```

count

Default: 40

Specifies the maximum number of servers that can be spawned in any 60 second interval. count must be a value in the range from 1 to 100.

**Usage**

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true as well in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

**Example**

```
max servers 50
```
Chapter 198
TFTP Configuration Mode Commands

The TFTP configuration mode is used to manage the TFTP servers for the current context.

```
Exec Mode
  configure
    Global Configuration Mode
      context name
        Context Configuration Mode
          server tftpd
            TFTP Configuration Mode
```
end

Exits the TFTP server configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the TFTP server configuration mode and returns to the context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Return to the context configuration mode.
max servers

Configures the maximum number of TFTP servers that can be started within any 60 second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product
All

Privilege
Security Administrator, Administrator

Syntax

max servers count

count

Default: 40

Specifies the maximum number of servers that can be spawned in any 60 second interval. count must be a value in the range from 1 to 100.

Usage

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true as well in that a system can benefit by reducing the number of servers such that TFTP services do not cause excessive system impact to other services.

Example

max servers 50
Chapter 199
Timedef Configuration Mode Commands

The Timedef Configuration Mode enables configuring the Time-of-Day Activation/Deactivation feature.

**Important:** This configuration mode is only available in StarOS 8.1 and StarOS 9.0 and later releases.

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

This command returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to change to the Exec mode.
exit

This command exits the current configuration mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.
**start**

This command configures timeslots in the current timedef.

---

**Important**: This command is only available in StarOS 8.1 and StarOS 9.0 and later releases.

**Important**: A maximum of 24 timeslots can be specified within a timedef.

---

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
[ no ] start day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time hh mm ss end day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time hh mm ss

[ no ] start time hh mm ss end time hh mm ss
```

---

**no**

Removes the specified timeslot.

---

**start day**

Specifies a timeslot with a start day and time, and an end day and time.

**start day**: Specifies the start day and start time.

**end day**: Specifies the end day and end time.

**time**

`hh mm ss`: Specifies the start/end time:

- `hh`: Specifies the start/end hour, and must be an integer from 0 through 23.
- `mm`: Specifies the start/end minute, and must be an integer from 0 through 59.
- `ss`: Specifies the start/end second, and must be an integer from 0 through 59.

---

**start time**

Specifies a timeslot with a start time and an end time to be applicable for all days of the week.

In specifying the start/end time:

- `hh`: Specifies the start/end hour, and must be an integer from 0 through 23.
- `mm`: Specifies the start/end minute, and must be an integer from 0 through 59.
- `ss`: Specifies the start/end second, and must be an integer from 0 through 59.

---

**Usage**

"Cisco ASR 5000 Series Command Line Interface Reference"
Use this command to create timeslots in a timedef during which rules have to be active. Timedefs enable activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only when they are active.

When a packet is received, and a ruledef/group-of-ruledefs is eligible for rule matching, if a timedef is associated with the ruledef/group-of-ruledefs, before rule matching, the packet-arrival time is compared with the timeslots configured in the timedef. If the packet arrived in any of the timeslots configured in the associated timedef, rule matching is undertaken, else the next ruledef/group-of-ruledefs is considered.

**Important:** The time considered for timedef matching is the system’s local time.

This release does not support configuring a timeslot for a specific date.

If, in a timeslot, only the time is specified, that timeslot will be applicable for all days.

If for a timeslot, “start time” > “end time”, that rule will span the midnight. I.e. that rule is considered to be active from the current day till the next day.

If for a timeslot, “start day” > “end day”, that rule will span over the current week till the end day in the next week.

In the following cases a rule will be active all the time:

- a timedef is not configured in an action priority
- a timedef is configured in an action priority, but the named timedef is not defined
- a timedef is defined but with no timeslots

**Example**

The following example specifies a timeslot that starts on Tuesday at 09:00:00 and ends on Friday 21:30:00:

```
start day tuesday time 9 0 0 end day friday time 21 30 0
```

The following example specifies a timeslot that starts at 15:00:00 and ends at 17:00:00 on all days of the week:

```
start time 15 0 0 end time 17 0 0
```

The following example specifies a timeslot that starts on Friday at 22:00:00 and ends on Tuesday at 08:00:00. This timeslot spans the complete week until the end day, i.e. up to Tuesday.

```
start day friday time 22 0 0 end day tuesday time 8 0 0
```

The following example specifies a timeslot that starts at 16:00:00 and ends at 09:00:00 on all days of the week. Also, as start time > end time, this timeslot spans the midnight too. I.e., from 16:00:00 to 23:59:59 and from 00:00:00 to 09:00:00.

```
start time 16 0 0 end time 9 0 0
```
Policy-Group is used to form a set of configured Policy-Maps for Traffic Policy feature. It applies multiple policies for a subscriber session flow within a destination context.

```
Exec Mode
    configure
    Global Configuration Mode
        context name
        Context Configuration Mode
        policy-group name name
        Traffic Policy Group Configuration Mode
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
**exit**

Exits the context configuration mode and returns to the global configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the global configuration mode.
policy

This command assigns the traffic policies, pre-configured in Policy-Map configuration mode, to a Policy Group for flow-based traffic policing to a subscriber session flow.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
[ no ] policy policy_map_name precedence value direction [ in | out ]
```

- **no**
  - Disables/removes configured policy for traffic policing.

- **direction [ in | out ]**
  - Specifies the direction in which the policies need to be applied.

- **policy_map_name**
  - Specifies the name of Policy-Map configured within a context to this policy group. A maximum of 16 policies can be assigned in a policy group.

- **precedence value**
  - Specifies the precedence of traffic policies to resolve. 
    - **value** is an integer in the range from 1 through 16. If a session flow matches multiple policies this keyword resolves them.

Usage
- Use this command to form a policy-group with a set of pre-configured Policy-Maps.

Example
- The following commands assigns the traffic policy policymap1 with precedence 2.
  
  ```
  policy policymap1 precedence 2
  ```
Chapter 201
Traffic Policy-Map Configuration Mode Commands

Policy-Map is used to configure a flow-based traffic policy for Traffic Policy feature within a destination context. It designates the flow treatment based on the classification rules configured in Class-Map mode for a subscriber session flow.
3gpp2 data-over-signaling

This command configures 3GPP2 related flow treatment policy for the flow-based traffic policing to subscriber session.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

[ no ] 3gpp2 data-over-signaling marking

no
Disables configured 3GPP2 related flow treatment policy.

marking
Indicates 3GPP2 related traffic flow for data over signaling channel.

Usage
Use this command to mark traffic flows for 3GPP2 related policy.

Example
3gpp2 data-over-signaling marking
access-control

This command configures the access control action for traffic flow matching with Class-Map rules.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
access-control { allow | discard }
```

- **allow**
  This option allows the packets, if policy matches with the criteria defined in Class-Map assigned to the specific traffic policy.

- **discard**
  This option discards the packets, if policy matches with the criteria defined in Class-Map assigned to the specific traffic policy.

**Usage**

Configures the action or treatment for traffic flows matching with criteria specified in assigned Class-Map.

**Example**
The following command allows the packets or traffic flow on matching with criteria specified in assigned Class-Map for specific traffic policy.

```
access-control allow
```
accounting suppress

This command suppresses accounting action on traffic flow matching the policy map.

Product
PDSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

[ no ] accounting suppress

no
Removes the suppression of accounting for traffic flow matching this policy map.

Usage
Use this command to suppress accounting action on traffic flow matching this policy map. Policy maps configured for accounting suppression are used to implement the QChat Billing Suppression feature to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. See the accounting trigger command.

Example
The following command configures suppression of accounting on traffic flows matching this policy map:

accounting suppress
accounting trigger

This command configures an accounting trigger policy map to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting to support the QCHAT Billing Suppression feature.

Product
PDSN

Privilege
Security Administrator, Administrator

Syntax

[ no | default ] accounting trigger { inactivity-timeout | interesting-traffic | intra-service-handoff }

default
Sets / Restores default value assigned for specified parameter.

no
Disables previously configured triggers.

inactivity-timeout
Generates an accounting stop message if there has been no data activity on the session for the interim accounting timeout interval.
Default: disabled

interesting-traffic
Generates an accounting start message upon arrival of interesting traffic.
Default: disabled

intra-service-handoff
Generates accounting start and stop messages during intra service handoffs within the same service.
Default: enabled
If this is disabled, the messages are suppressed during the handoffs. The current accounting session continues and no stop or start messages are generated during the intra service handoff.

Usage

Use this command to configure an accounting trigger policy map (ATPM) to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting to support the QChat Billing Suppression feature.
Interesting traffic is identified as traffic that does not match any of the other Accounting Policy Maps (APMs) configured for accounting suppression. See the `accounting suppress` command.
An ATPM is similar to an APM, but without the class map rules. The ATPM is configured as of type accounting using the `type accounting` command.
In the ATPM, the trigger to start accounting for interesting traffic is configured using the `accounting trigger interesting-traffic` command. Accounting Start is triggered on arrival of interesting traffic, or change in airlink parameters conveyed through active-start airlink record. If an active-start record was included in the initial connection setup, Accounting Start is not triggered. But if the active-start comes separately and is the first one for the session, it is treated as airlink change and an Accounting Start is sent. Optionally, timeout can be triggered when there is no data traffic for the interim accounting timeout interval using the `accounting trigger inactivity-timeout stop` command. On timeout, the accounting session is terminated and an Accounting Stop message is sent. A new accounting session is created if interesting traffic resumes.

The ATPM should have the lowest precedence among the APMs. As the airlink events are generated on the ingress side, the ATPM must be included in a policy group that is applied to the ingress direction in the subscriber profile. The configuration is applicable only for standard trigger policy and session based accounting mode.

**Example**
The following command sets the trigger to generate accounting start message upon arrival of interesting traffic:

```
accounting trigger interesting-traffic
```
class-map

This command assigns a traffic classification rule (Class-Map) to the policy map.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
    class-map name
```

`name`

Specifies the name of the class map assigned for this policy map. The class map should be one that was configured in the Class Map Configuration Mode.

`name` must be the name of a class map, and must be a string of 1 through 15 characters in length.

**Usage**
Use this command to assigns a class map to the policy map for traffic policing. The class map is configured in the Class Map Configuration Mode.

**Example**
The following command assigns the class map classification1 to the current policy map:

```
class classification1
```
end

This command exits the current mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
exit

This command exits the current mode and returns to the parent mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent mode.
flow-tp-trigger

This command specifies that the traffic volume will be calculated based on the traffic on the flow.

Product
PDSN, HA, ASN GW

Privilege
Security Administrator, Administrator

Syntax

flow-tp-trigger volume

no flow-tp-trigger volume

    volume
    Specifies the volume threshold to trigger traffic policing.
    volume is the value in bytes, and must be an integer from 1 through 4294967295.

Usage
This command is available if you have purchased and installed the Intelligent Traffic Control License on your system. Use this command to calculate the traffic volume based on the traffic on the flow.

Example

flow-tp-trigger 500
ip header-compression

Enables the system to mark IP flows for RObust Header Compression.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] ip header-compression rohc flow-marking
```

- **no**
  Disables the setting.

- **rohc flow-marking**
  Marks the IP flow for SO67 and PPP ROHC.

**Usage**

Use this command to mark IP flows for SO67 and PPP ROHC.

**Example**

```
ip header-compression rohc flow-marking
```
qos encaps-header

Enables and configures Quality of Service (QoS) policy to use Differentiated Service Code Point (DSCP) marking in IP header field for the flow-based traffic policing to subscriber session flow.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**
```
qos encaps-header dscp-marking ( dscp_code | copy-from-user-datagram | ignore-pcf-signaled-dscp | user-datagram )
```

- **dscp_code**
  Specifies the DSCP code value marked in IP header of packet/flow to determine the QoS for traffic policing. The value must be expressed as a hexadecimal value from 0x00 through 0x3F.

- **copy-from-user-datagram**
  Specifies to use DSCP code value from user datagram (UDP header) to determine the QoS for traffic policing.

- **ignore-pcf-signaled-dscp**
  Specifies to override the highest priority DSCP value signaled by the PCF.

- **user-datagram**
  Specifies to use the DSCP value copied from the user datagram.

**Usage**
Use this command to apply the QoS policy based on DSCP code value encapsulated in IP packet header or User datagram packet to subscriber session flow for flow-based traffic policing.

**Important**: Details on the QoS traffic policing functionality is located in the System Administration and Configuration Guide.

**Example**
The following command sets QoS policy with DSCP code value to 0x0C for Class 1, silver (AF12):
```
qos encaps-header dscp-marking 0x0C
```
qos traffic-police

Enables and configures Quality of Service (QoS) policy for the flow-based traffic policing to subscriber session flow on per-flow basis.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
qos traffic-police committed bps peak bps burst-size bytes exceed-action { drop | lower-ip-precedence | allow } violate-action { drop | lower-ip-precedence | allow }

burst-size bytes
Default: 3000
The peak burst size allowed, in bytes.
bytes must be an integer from 0 through 4294967295.
```

**Important:** It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

```plaintext
committed bps
Default: 144000
The committed data rate (guaranteed-data-rate) in bps (bits per second).
bps must be an integer from 0 through 4294967295.
```

```plaintext
exceed-action { drop | lower-ip-precedence | allow }
Default: lower-ip-precedence
The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate.
The following actions are supported:
drop: Drop the packet
lower-ip-precedence: Transmit the packet after lowering the ip-precedence
allow: Transmit the packet
```

```plaintext
peak bps
Default: 256000
Specifies the peak data-rate for the subscriber, in bps (bits per second).
bps must be an integer from 0 through 4294967295.
```

```plaintext
violate-action { drop | lower-ip-precedence | allow }
Default: drop
The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
drop: Drop the packet
```
**qsos traffic-policy**

**lower-ip-precedence**: Transmit the packet after lowering the IP precedence

**allow**: Transmit the packet

---

**Usage**

Use this command to apply the QoS policy to subscriber session flow for flow-based traffic policing.

---

**Important**: Details on the QoS traffic policing functionality are located in the System Administration.

---

**Example**

The following command sets committed data rate of 102400 bps with peak data rate of 128000 bps and burst size 2048 bytes. This lowers the IP precedence when the committed-data-rate exceeded and drops the packets when peak-data-rate are violated:

```
qos traffic-policy committed 102400 peak-data-rate 128000 burst-size 2048 exceed-action lower-ip-precedence violate-action drop
```
**qos user-datagram dscp-marking**

Enables and configures Quality of Service (QoS) policy related to differentiated service code point (DSCP) marking in user datagram of subscriber session flow on per-flow basis.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
qos user-datagram dscp-marking dscp_code
```

*dscp_code*

Specifies the DSCP code value marked in IP header of packet/flow to determine the QoS for traffic policing. The value must be expressed as a hexadecimal value from 0x00 through 0x3F.

**Usage**

Use this command to apply the QoS policy to subscriber session flow by DSCP marking in user datagram.

**Example**
The following command sets DSCP marking for user datagram as 0x01 for QoS to subscriber session flow:

```
qos user-datagram dscp-marking 0x01
```
**sess-tp-trigger**

This command configures the trigger traffic control based on traffic volume on a session.

**Product**
PDSN, HA, ASN GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sess-tp-trigger volume
```

```
no sess-tp-trigger volume
```

*volume*

Specifies the traffic volume threshold to trigger traffic control. *volume* is a value in bytes from 1 to 4294967295.

**Usage**

This command is available if you have purchased and installed the Intelligent Traffic Control License on your system. Use this command to configure the trigger traffic control based on traffic volume on a session.

**Example**

```
sess-tp-trigger 500
```
**type**

This command specifies the type of traffic policy within specific Policy-Map.

**Product**
PDSN, HA, ASN GW

**Privilege**
Administrator

**Syntax**

```
type { accounting | dynamic ( three-gpp2 rev-A profile-id { any | id profile_id | range low_value to high_value } flow-id { any | id flow_id | range low_value to high_value } | pre-provisioned wimax asn-service-profile-id { any | id service_id } asn-pdfid { any | id pdf_id } | static | template }
```

**accounting**
Specifies the type of traffic policing as accounting for this specific policy map. This configuration is used for enabling/disabling the accounting of different flows matching with conditions within this Policy-Map.

**dynamic**
Identifies the type of policy map as dynamic.

**three-gpp2 rev-A**
Configures dynamic policy map type for CDMA2000-3GPP2 RevA service.

**profile-id { any | id profile_id | range low_hex to high_hex }**
Specifies the profile id matching in this policy map.

- **any** allows any profile identifier matching with in this policy map.
- **id profile_id** allows specific profile identifier matching with in this policy map. `profile_id` must be either a value in hexadecimal format from 0x0 to 0xFFFF or an integer from 0 to 65535.
- **range low_value to high_value** identifies a range in which a profile identifier must fall within to be considered a match. `low_value` and `high_value` must be either a value in hexadecimal format from 0x0 to 0xFFFF or an integer from 0 to 65535.

**flow-id { any | id flow_id | range low_hex to high_hex }**
Specifies the flow id matching in this policy map.

- **any** allows any flow identifier matching with in this policy map.
- **id flow_id** allows specific flow identifier matching with in this policy map. `flow_id` must be either a value in hexadecimal format from 0x0 to 0xFFFF or an integer from 0 to 65535.
- **range low_value to high_value** identifies a range in which a flow identifier must fall within to be considered a match. `low_value` and `high_value` must be either a value in hexadecimal format from 0x0 to 0xFFFF or an integer from 0 to 65535.

**pre-provisioned**
Identifies the type of policy map as pre-provisioned.
Traffic Policy-Map Configuration Mode Commands

⚠️

Cisco ASR 5000 Series Command Line Interface Reference

Traffic Policy

- Map Configuration

- Mode Commands

vic

Configures WiMAX service policy map in an ASN-GW service.

asn-service-profile { any | id service_id }

- Specifies the ASN Service profile identifier to match with in this policy map.
- `any`: Allows any ASN Service Profile Identifier matching within this policy map.
- `id service_id`: Allows specific Service Profile matching to a specified identifier. `service_id` must be an integer from 1 to 65535 and must match a service ID that was configured in the Subscriber Configuration Mode.

asn-pdfid { any | id pdf_id }

- Specifies the ASN Packet Data Flow Identifier to match with in this policy map.
- `any`: Allows any ASN Packet Data Flow Identifier matching within this policy map.
- `id pdf_id`: Allows specific Packet Data Flow matching to a specified identifier. `pdf_id` must be an integer from 1 to 255 and must match a PDF ID that was configured in the Subscriber Configuration Mode.

static

- Specifies the type of traffic policing as static for this specific Policy Map. In this type of policy, the traffic flow classification and flow treatment is pre-defined with classification rules through Class-Map configuration.
- This is the detailed type of policy map.

template

- Specifies the type of traffic policy to as a template to all subscribers associated with this policy map.

Usage

- Specifies the type of traffic policy within the specific Policy-Map.

Example

- The following commands configures the traffic policy for this Policy-Map as static:
  - `type static`
- The following commands configures the traffic policy for this Policy-Map as pre-provisioned for WiMAX service requiring a match of any service profile and PDF id of 3:
  - `type pre-provisioned wimax asn-service-profile any asn-pdfid id 3`
Chapter 202
Tunnel Interface Configuration Mode Commands

The Tunnel Interface Configuration Mode is used to create and manage the IP interfaces for various type of tunnels and its parameters like addresses, address resolution options, etc.

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

Configures the description text for the current interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

description <text>

no description

- **no**
  
  Clears the description for the interface.

- **text**
  
  Specifies the descriptive text to use. *text* must be 0 to 79 alpha and/or numeric characters with no spaces or a quoted string of printable characters. The interface description is case sensitive.

**Usage**

Set the description to provide useful information on the interface’s primary function, services, end users, etc. Any information useful may be provided.

**Example**

Following command sets the description about this interface:

```bash
description sampleInterfaceDescriptiveText
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the Interface Configuration Mode and returns to the Context Configuration Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
ip address

This command configures the IPv4 address for the specific tunnel interface.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
ip address [ip_address/ip_mask | ip_address ip_mask]
```

```
o ip address ip_address
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured IPv4 address bound to a tunnel interface.</td>
</tr>
</tbody>
</table>

```
[ip_address/ip_mask | ip_address ip_mask]
```

| Specifies a destination IP address or group of addresses that will use this route. |

```
ip_address/ip_mask: Specifies a combined IP address subnet mask bits to indicate what IP addresses are included in the route. ip_address/ip_mask must be specified using the form ‘IP Address/Mask Bits’ where the IP address is specified using the standard IPv4 dotted decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask. |
```

```
ip_address ip_mask: Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. ip_address must be specified using the standard IPv4 dotted decimal notation. ip_mask must be specified using the standard IPv4 dotted decimal notation as network mask for subnets. The mask as specified by ip_mask or resulting from ip_address/ip_mask is used to determine the network for packet routing. 0’s in the resulting mask indicate the corresponding bit in the IP address is not significant in determining the network for packet routing. 1’s in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network. |
```

Usage

Use this command to bind the IPv4 address to a tunnel interface. This address does not affect the encapsulation of packets going out on the tunnel interface.

Example

The following command will assign the 1.2.3.4 as IPv4 address to this tunnel interface:

```
ip address 1.2.3.4
```
**ipv6 address**

This command configures the IPv6 address for the specific tunnel interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
ipv6 address ipv6_address/ipv6_mask
no ipv6 address ipv6_address
```

**no**

Removes the configured IPv6 address bound to a tunnel interface.

```
ipv6_address/ipv6_mask
```

Specifies a destination IP address or group of addresses that will use this route. `ipv6_address/ipv6_mask`: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. `ipv6_address/ipv6_mask` must be specified using the form ‘IP Address/Mask Bits’ where the IP address is specified using the standard IPv4 dotted decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

**Usage**

Use this command to bind the IPv6 address to a tunnel interface. This address does not affect the encapsulation of packets going out on the tunnel interface.

**Example**

The following command will assign the `1001::2:010:1234` as IPv4 address to this tunnel interface:

```
ipv6 address 1001::2:010:1234
```
tunnel-mode

This command configures the tunnel mode type for specific tunnel interface. It also creates the specific tunnel configuration mode if required.

Product
All

Privilege
Security Administrator, Administrator

Syntax

tunnel-mode {gre | ipv6ip}
default tunnel-mode

default
Sets the default tunnel mode for this interface. By default tunnel mode is set to IPv6-to-IPv4 type.

gre
Default: Disabled
This keyword sets the tunnel interface mode to GRE type and creates the GRE tunnel Configuration mode if required.

ipv6ip
Default: Enabled
This keyword sets the tunnel interface mode to IPv6-to-IPv4 type and creates the IPv6-to-IPv4 Tunnel Configuration mode, if required.

Usage
Use this command to set the tunnel mode type of GRE or IPv6-to-IPv4 for tunneling interface.

Example
The following command sets the tunnel mode to GRE for specific interface:

    tunnel-mode gre
Chapter 203
UDR Format Configuration Mode Commands

The UDR Configuration Mode enables configuring User Detail Record (UDR) formats. UDR file formats are represented in Comma Separated Value (CSV).

<table>
<thead>
<tr>
<th>Exec Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-charging service name</td>
</tr>
<tr>
<td>ACS Configuration Mode</td>
</tr>
<tr>
<td>udr-format name</td>
</tr>
<tr>
<td>UDR Format Configuration Mode</td>
</tr>
</tbody>
</table>

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

This command specifies the order of fields in the UDR.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
```

```
o attribute attribute [ priority priority ]
```

- **no**
  - Removes the specified attribute configuration.

- **attribute**
  - Specifies the attribute.
  - `attribute` must be one of the following:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter-session-id</td>
<td>Unique Diameter session identifier.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in Release 8.3 and later releases.</td>
</tr>
<tr>
<td>radius-called-station-id</td>
<td>Called Station ID of the mobile handling the flow.</td>
</tr>
<tr>
<td>radius-calling-station-id</td>
<td>Calling Station ID of the mobile handling the flow.</td>
</tr>
<tr>
<td>radius-fa-nas-identifier</td>
<td>RADIUS NAS identifier of Foreign Agent (FA).</td>
</tr>
<tr>
<td>radius-fa-nas-ip-address</td>
<td>RADIUS IP address of Foreign Agent (FA).</td>
</tr>
<tr>
<td>radius-nas-identifier</td>
<td>RADIUS NAS identifier.</td>
</tr>
<tr>
<td>radius-nas-ip-address</td>
<td>RADIUS NAS IP address.</td>
</tr>
<tr>
<td>radius-user-name</td>
<td>User name associated with the flow.</td>
</tr>
<tr>
<td>sn-3gpp2-bsid</td>
<td>This option is obsolete. To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sn-3gpp2-carrier-id</td>
<td>This option is obsolete. To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-3gpp2-esn</td>
<td>This option is obsolete. To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-3gpp2-meid</td>
<td>This option is obsolete. To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-3gpp2-service-option</td>
<td>This option is obsolete. To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-acct-beginning-session</td>
<td>Session beginning information. Important: This attribute is customer specific, and is only available in Release 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-acct-session-continue</td>
<td>Session continue information. Important: This attribute is customer specific, and is only available in Release 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-acct-session-id</td>
<td>Indicator for the accounting session Identifier.</td>
</tr>
<tr>
<td>sn-acct-session-time</td>
<td>Duration from acct-status-type:start to acct-status-type:stop. Important: This attribute is customer specific, and is only available in Release 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-acct-status-type</td>
<td>Accounting status identifier. Important: This attribute is customer specific, and is only available in Release 8.3 and later releases.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sn-charging-type</td>
<td>Charging type:</td>
</tr>
<tr>
<td></td>
<td>- offline</td>
</tr>
<tr>
<td></td>
<td>- online</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>: This attribute is customer specific, and is only available in Release 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-closure-reason</td>
<td>Includes reason for the termination of the flow/UDR:</td>
</tr>
<tr>
<td></td>
<td>- 0: normal, i.e., subscriber session ended</td>
</tr>
<tr>
<td></td>
<td>- 1: handoff control processing specified</td>
</tr>
<tr>
<td></td>
<td>- 2: subscriber session terminated</td>
</tr>
<tr>
<td></td>
<td>- 3: flow timeout</td>
</tr>
<tr>
<td>sn-content-id</td>
<td>Unique identifier for the content-id.</td>
</tr>
<tr>
<td>sn-content-label</td>
<td>Identifier for text label for content-id.</td>
</tr>
<tr>
<td>sn-content-vol</td>
<td>Identifier for content volume.</td>
</tr>
<tr>
<td>sn-correlation-id</td>
<td>RADIUS correlation identifier.</td>
</tr>
<tr>
<td>sn-duration</td>
<td>Duration between the last and first packet for the record.</td>
</tr>
<tr>
<td>sn-end-time [ format ]</td>
<td>Timestamp for last packet of flow in UTC.</td>
</tr>
<tr>
<td></td>
<td>[ format ]</td>
</tr>
<tr>
<td>sn-fa-correlation-id</td>
<td>RADIUS Correlation Identifier of the Foreign Agent (FA).</td>
</tr>
<tr>
<td>sn-fa-ip-address</td>
<td>FA IP address.</td>
</tr>
<tr>
<td>sn-filler-blank</td>
<td>Keeps attributes place blank and generates an empty UDR field.</td>
</tr>
<tr>
<td>sn-filler-zero</td>
<td>Fills ‘0’ for this attribute place in the EDR/UDR.</td>
</tr>
<tr>
<td>sn-format-name</td>
<td>Indicates the name of the UDR/EDR format used.</td>
</tr>
<tr>
<td>sn-group-id</td>
<td>Indicates the sequence group identifier for the records.</td>
</tr>
<tr>
<td>sn-ha-ip-address</td>
<td>Home Agent IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>: This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-local-seq-no</td>
<td>Unique local sequence number of UDR identifier per ACSMgr and linearly increasing in UDR file.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sn-ocs-ip-address</td>
<td>Online Charging Server's IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in</td>
</tr>
<tr>
<td></td>
<td>Release 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-rulebase</td>
<td>Indicates the name of the ACS rulebase used.</td>
</tr>
<tr>
<td>sn-sequence-no</td>
<td>Unique sequence number (per <code>sn-sequence-group</code> and <code>radius-nas-ip-address</code>)</td>
</tr>
<tr>
<td></td>
<td>of UDR identifier and linearly increasing in UDR file.</td>
</tr>
<tr>
<td>sn-served-bsa-addr</td>
<td>Indicator for address of Base Station Area being served.</td>
</tr>
<tr>
<td>sn-service-name</td>
<td>Indicator for ACS service name.</td>
</tr>
<tr>
<td>sn-st16-ip-addr</td>
<td>IP address of the chassis handling this flow.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is interchangeable with <code>radius-nas-ip-address</code> for other systems.</td>
</tr>
<tr>
<td>sn-start-time [ format ]</td>
<td>Timestamp for first packet of flow in UTC.</td>
</tr>
<tr>
<td>sn-stream-number</td>
<td>Unique UDR billing record identifier.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in</td>
</tr>
<tr>
<td></td>
<td>Release 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-subscriber-id</td>
<td>Indicator for subscriber ID.</td>
</tr>
<tr>
<td>sn-subscriber-nat-flow-ip</td>
<td>NAT IP address(es) of NAT-enabled subscriber.</td>
</tr>
<tr>
<td>sn-timestamp</td>
<td>Timestamp when the UDR is actually generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in</td>
</tr>
<tr>
<td></td>
<td>Release 8.3 and later releases.</td>
</tr>
</tbody>
</table>


Specifies the timestamp format.


**localtime**

Specifies the local time. By default, timestamps are displayed in GMT.

```plaintext
{ bytes | pkts } { downlink | uplink }
```

Specifies bytes/packets sent/received from/by mobile.

**priority priority**

Specifies the position priority of the value within the UDR. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first.

*priority* must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

**Usage**

Use this command to set the attributes and priority for UDR file format.

A particular field in UDR format can be entered multiple times at different priorities. While removing the UDR field using the `no attribute` command either you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional *priority* keyword.

**Example**

```plaintext
attribute radius-user-name priority 12
```
end

This command returns the CLI prompt to the Exec mode.

Product
- All

Privilege
- Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to change to the Exec mode.
event-label

This command configures an optional event ID to use in generated billing records.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
event-label label priority priority
no event-label
```

- **no**
  Removes the previously configured event label for UDR attribute.

- **label**
  Specifies event label for attribute to be used for UDR format.
  *label* must be an alpha and/or numeric string of 1 through 63 characters in length.

- **priority priority**
  Specifies the CSV position of event ID in UDR.
  *priority* must be an integer from 1 through 65535.

**Usage**

Use this command to set the event ID and its position in UDR file format.

**Example**

```
event-label radius_csv1 priority 23
```
exit

This command exits the UDR Format Configuration Mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
rule-variable

This command specifies the order of fields in the UDR.

Product
All

Privilege
Security Administrator, Administrator

Syntax

rule-variable protocol rule priority priority

no rule-variable [ priority priority ] protocol rule

removes the rule-variable protocol configuration.

protocol rule

Specifies the rule variable for UDR format.

protocol must be one of the following with specified rule:

• bearer 3gpp2: Bearer-related configuration:

  • always-on
  • bsid
  • carrier-id
  • esn
  • ip-qos
  • ip-technology
  • meid
  • release-indicator
  • serv-MDN
  • service-option
  • session-begin
  • session-continue

**Important:** For more information on protocol-based rules see the Ruledef Configuration Mode Commands chapter.

priority priority

Specifies the CSV position of the value in the UDR.

priority must be an integer from 1 through 65535.
Usage
Use this command to set the rule variables priority for UDR file format.
A particular field in UDR format can be entered multiple times at different priorities. While removing the
UDR field using the `no rule-variable` command either you can remove all occurrences of a particular
field by specifying the field name or a single occurrence by additionally specifying the optional priority
keyword.

Example
```
rule-variable bearer 3gpp2 bsid priority 36
```
Chapter 204
UDR Module Configuration Mode Commands

To access the UDR Module Configuration Mode, in the Context Configuration Mode, enter the udr-module active-charging-service command.

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

This command configures the EDR/UDR file parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```plaintext
cdr [ push-interval value ] [ push-trigger space-usage-percent trigger_percentage ] [ remove-file-after-transfer ] [ transfer-mode { pull | push primary { encrypted-url enc_url | url url } [ via local-context ] [ secondary { encrypted-secondary-url enc_sec_url | url sec_url } ] } ] + | use-harddisk ]
```

```plaintext
no cdr [ remove-file-after-transfer | use-harddisk ] +
```

```plaintext
default cdr [ push-interval | push-trigger space-usage-percent | remove-file-
after-transfer | transfer-mode [ push via ] | use-harddisk ] +
```

```plaintext
no
```

Disables the configured CDR storage and CDR file processing in this mode:

- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the SMC harddisk.

**Important**: `use-harddisk` keyword is available only on the ASR 5000 chassis.

**Important**: `use-harddisk` keyword is only available on ASR 5000 chassis.

```plaintext
push-interval value
```

Default: 300

Specifies the transfer interval, in seconds, to push EDR and UDR files to an external file server.
value must be an integer from 60 through 3600.

push-trigger space-usage-percent trigger_percentage

Default: 80%
Specifies the EDR/UDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server. trigger_percentage specifies the EDR/UDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.

remove-file-after-transfer

Default: Disabled
Specifies that the system must delete EDR/UDR files after they are transferred to the external file server.

transfer-mode { pull | push primary [ encrypted-url enc_url | url url ] [ via local-context ] [ secondary [ encrypted-secondary-url enc_sec_url | secondary-url sec_url ] ] }

Specifies the EDR/UDR file transfer mode.
- pull: Specifies that the L-ESS is to pull the CDR files.
- push: Specifies that the system is to push CDR files to the configured L-ESS.
- primary encrypted-url enc_url: Specifies the primary URL location in encrypted format to which the system pushes the CDR files. enc_url must be the location name in an encrypted format, and must be an alpha and/or numeric string of 1 through 1024 characters in length.
- primary url url: Specifies the primary URL location to which the system pushes the CDR files. url must be an alpha and/or numeric string of 1 through 1024 characters in the //user:password@host:[port]/directory format.
- via local-context: Configuration to select LC/SPIO for transfer of CDRs. The system pushes the UDR files via SPIO in the local context.
- encrypted-secondary-url enc_sec_url: Specifies the secondary URL location in encrypted format to which the system pushes the CDR files when the primary location is unreachable or fails. enc_sec_url must be the location name in an encrypted format, and must be an alpha and/or numeric string of 1 through 1024 characters in length.
- secondary-url sec_url: Specifies the secondary URL location to which the system pushes the CDR files when the primary location is unreachable or fails. sec_url must be an alpha and/or numeric string of 1 through 1024 characters in //user:password@host:[port]/directory format.

use-harddisk

Default: Disabled
Specifies that on ASR 5000 chassis the hard disk on the SMC be used to store EDR/UDR files. On configuring to use the hard disk for EDR/UDR storage, EDR/UDR files are transferred from RAMFS on the PSC to the hard disk on the SMC.

Important: use-harddisk keyword is available only on the ASR 5000 chassis.

+ Indicates that more than one of the previous keywords can be entered within a single command.
Usage

Use this command to configure how charging data records (CDR) are moved and stored.

On the ASR 5000 chassis, run this command only from the local context. Running in any other context would fail and deliver an error message.

The **use-harddisk** keyword is only available on the ASR 5000 system. This command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message “Failure: Please Check if CDRMOD is running in this context or not.”

This config can be applied either in the EDR/UDR module, but will be applicable both to the EDR and UDR modules. Configuring in one of the modules prevents the configuration to be done in the other module.

If PUSH transfer mode is selected, the L-ESS server URL to which the CDR files need to be transferred must be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur
- After switching from the primary server, 30 minutes elapses

When changing **transfer-mode** from pull to push, disable the PULL from L-ESS and then change the transfer mode to push. Make sure that the push server URL configured is accessible from the local context. Also, make sure that the base directory that is mentioned contains udr directory created within it.

When changing **transfer-mode** from push to pull, after changing, enable PULL on the L-ESS. Any of the ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH activity going on at the time of this configuration change, all the PUSH related configuration is nullified immediately.

Example

The following command configures the system to retain a copy of the data file after it has been transferred to the storage location:

```
no cdr remove-file-after-transfer
```
end

This command returns the CLI prompt to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to change to the Exec mode.
exit

This command exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
file

This command sets UDR file parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
default file [ charging-service-name ] [ compression ] [ current-prefix ] [ delete-timeout ] [ directory ] [ field-separator ] [ file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [ rotation { num-records | time | volume } ] [ sequence-number ] [ storage-limit ] [ time-stamp ] [ trailing-text ] [ udr-seq-num ]
```

---

**default**
Using default file will reset some but not all keyword parameters to their default values. To ensure that the default is reset for a specific parameter, include the keyword in the default file syntax.

---

**charging-service-name { include | omit }**
Configures the inclusion and exclusion of charging service name in the file name.
Default: include
- **include**: Sets this command to include the Charging service name in UDR file name.
- **omit**: Sets this command to exclude or omit the Charging service name from UDR file name.

---

**compression { gzip | none }**
Configures the compression of the UDR file.
Default: none
- **gzip**: Enables GNU zip compression of the UDR file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

---

**current-prefix string**
Default: curr
Specifies a string to add to the beginning of the UDR file that is currently being used to store UDR records.
*string* must be an alpha and/or numeric string of 1 through 31 characters in length.

---

**delete-timeout seconds**
Default: Disabled
Specifies a time period, in seconds, when completed UDR files are deleted. By default, files are never deleted. *seconds* must be an integer from 3600 through 31536000.

---

**directory dir_name**
Default: /records/udr
Specifications a subdirectory in the default directory in which to store UDR files. `dir_name` must be an alpha and/or numeric string of 1 through 191 characters in length.

**exclude-checksum-record**

Default: Disabled, inserts checksum record into the UDR file header. When entered, this keyword excludes the final record containing `#CHECKSUM` followed by the 32-bit cyclic redundancy check (CRC) of all preceding records from the UDR file.

**field-separator { hyphen | omit | underscore }**

Specifies the field separators between two fields of UDR file name. Default: underscore

- **hyphen**: specifies the field separator as `-' (hyphen) symbol between two fields.
- **omit**: removes or omits the field separator between two fields.
- **underscore**: specifies the field separator as `_' (underscore) symbol between two fields.

**file-sequence-number rulebase-seq-num**

Generates unique file sequence numbers for different rulebase-formatname combinations.

**headers**

Includes a file header summarizing the record layout.

**name file_name**

Default: udr

Specifies a string to use as the base file name for UDR files. `file_name` must be an alpha and/or numeric string of 1 through 31 characters in length. The file name format is as follows:

```
base_rulebase_format_sequencenum_timestamp
```

- **base**: Specifies type of record in file or contains the operator-specified string. Default is `udr`.
- **rulebase**: Specifies the name of the Rulebase. UDRs from different Rulebases go into different UDR files.
- **format**: Specifies the name of the UDR format if `single-udr-format` is specified else the format field (and the trailing underscore) is omitted from the file name.
- **sequencenum**: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all UDR files on the system.
- **timestamp**: Contains a timestamp based on file creation time in UTC time in MMDDYYYYHHMMSS format.

UDR files that have not been closed have a string added to the beginning of their file names. File name for a UDR file in CSV format that contains information for rule base named rulebase1 and a UDR schema named udr_schema1 appears as follows:

```
udr_rulebase1_udr_schema1_00005_01302006143409
```

If file name is not configured it creates files for EDRs/UDRs/FDRs (xDRs) having following name template with limits to 256 characters:

```
basename_ChargSvcName__timestamp_SeqNumResetIndicator_FileSeqNumber
```

- **basename**: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ECS.
ChargSvcName: A system context-based configurable text string that uniquely identifies a specific context-based charging service.

timestamp: Date and time at the instance of file creation. Date and time in the form of “MMDDYYHHmmSS” where HH is a 24-hour value from 00-23.

SeqNumResetIndicator: A one byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 through 255 which is incremented by a value of 1 for the following conditions:

Failure of an ECS software process on an individual PSC

Failure of the system such that a second system takes over (for example, a standby or backup chassis put in place according to Inter-chassis Session Recovery)

File Sequence Number (FileSeqNumber) rollover from 999999999 to 0

FileSeqNumber: unique file sequence number for the file with 9 digit integer having range from 000000000 to 999999999. It is unique on each chassis system.

File name for a closed xDR file in CSV format that contains information for ECS system xyz_city1 and charging service name prepaid2 with timestamp 12311969190000, and file sequence number counter reset indicator to 002 for file sequence number 034939002 appears as follows:

xyz_city1_preapaid2_12311969190000_002_034939002

File name for a running xDR file in CSV format that contains information for the same parameters for file sequence number 034939003 prefixed with curr_ and appears as follows:

curr_xyz_city1_preapaid2_12311969190000_002_034939002

reset-indicator

This option includes the reset indicator counter value from 0 to 255 in UDR file name and is incremented (by one) whenever any of the following conditions occur:

- An ACSMgr process fails
- A peer chassis has taken over in compliance with our Inter-chassis Session Recovery feature
- The sequence number-keyword has rolled over to zero

rotation { num-records records | time seconds | volume bytes }

Defaults:
num-records: 1024

time: 3600 seconds

volume: 102400 bytes

Specifies when to close a UDR file and create a new one.

num-records records: Specifies the number of records that should be added to the file. When the number of records in the file reaches the specified value, the file is complete. records must be an integer from 100 through 10240.

time seconds: Specifies the period of time to wait before closing the UDR file and creating a new one. seconds must be an integer from 30 through 86400.

volume bytes: Specifies the maximum size of the UDR file before closing it and creating a new one. bytes must be an integer from 51200 through 62914560. Note: Higher sets may provide the best compression ratio when the compression keyword is set to gzip.

sequence-number { length length | omit | padded | padded-six-length | unpadded }

Default: padded

Specifies including/excluding sequence number in the file name.
**length** *length*: Includes the sequence number with the specified length. *length* must be the file sequence number length with preceding zeroes in the file name, and must be an integer from 1 through 9.

**Important**: The **length** configuration is applicable in both EDR and UDR modules. When applied in both modules without the **file udr-seq-num** configuration, the minimum among the two values will come into effect for both the modules. With the **file udr-seq-num** config, each module will use its own value of length.

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

**storage-limit** *limit*

Default: 33554432

Specifies deleting files when the specified amount of space, in bytes, is used up for UDR/EDR file storage on the PSCs RAM.

On ASR 5000 chassis, *limit* is an integer from 10485760 through 536870912.

**Important**: On ASR 5000 chassis, the total storage limit is 536870912 bytes (512 MB). This limit is for both UDR and EDR files combined.

**time-stamp** { expanded-format | rotated-format | unix-format }

Specifies the timestamp of when the file was created be included in the file name.

- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of \( x.y \), where \( x \) is the number of seconds since 1/1/1970 and \( y \) is the fractional portion of the current second that has elapsed.

**trailing-text** *string*

Specifies the inclusion of arbitrary text string in the file name. *string* must be an alpha and/or numeric string of 1 through 30 characters in length.

**trap-on-file-delete**

Default: Disabled

This keyword instructs the system to send an SNMP notification (trap) when an EDR/UDR file is deleted due to lack of space.

**udr-seq-num**

Default: Disabled

Specifies that the file sequence numbers that are part of the UDR file names be independently generated. If disabled, a single set of sequence numbers are shared by both EDR files and UDRs.
file

xor-final-record
Default: Disabled
Specifies inserting an xor checksum (in place of the CRC checksum) into the UDR file header if the exclude-checksum-record keyword is left at its default setting.

More than one of the previous keywords can be entered within a single command.

Usage
Use this command to configure UDR file characteristics.

Example
The following command sets the prefix of the current active UDR file to current:

    file current-prefix current

The following command sets the base file name to UDRfile

    file name UDRfile
The VLAN Configuration Mode is used to create and manage Virtual LANs and their bindings between contexts.
**bind interface**

Configures a virtual interface to context association for the current VLAN.

**Product**
PDSN, HA, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
bind interface interface_name context_name
no bind interface interface_name context_name
```

`no`
Indicates the binding between the virtual interface specified and the context specified is to be unbound for the current VLAN.

`interface_name`
Specifies the name of the virtual interface to be bound to the context. `interface_name` must be from 1 to 79 alpha and/or numeric characters.

`context_name`
Specifies the name of the context to be bound to the virtual interface. `context_name` must refer to a previously configured context.

**Usage**
Bind a virtual interface and context to allow the VLAN to provide service.

**Example**

```
bind interface sampleVirtual sampleContext
no bind interface sampleVirtual sampleContext
```
end

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

**Product**
PDSN, HA

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the VLAN configuration mode and returns to the port configuration mode.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the port configuration mode.
**ingress-mode**

This command toggles between enabling and disabling the port ingress mode.

**Product**
PDSN, HA, SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
-ingress-mode
```

**Usage**
Use this command to enable or disable the ingress mode for the port.

**Example**

```
ingress-mode
```
shutdown

Disables/enables traffic over the current VLAN.

Product
PDSN, HA

Privilege
Security Administrator, Administrator

Syntax

```
shutdown
no shutdown
```

```
no
```

Enables the VLAN. When omitted the VLAN is shutdown.

Usage
Shut down a VLAN.
This command is necessary to bring a VLAN into service by enabling it via the `no` keyword.

Example
To disable a VLAN from sending or receiving network traffic use the following command:
```
shutdown
```
To enable a VLAN use the following command:
```
no shutdown
```
**vlan-map**

This command sets a single next-hop IP address so that multiple vlans can use a single next-hop gateway. `vlan-map` is associated with a specific interface.

**Product**
PDSN, HA, SGSN

**Privilege**
Security Administrator, Administrator

`vlan-map next-hop ip_address`

**Usage**
Use `vlan-map` to combine multiple vlan links to go through a single IP address. This feature is used in conjunction with nexthop forwarding and overlapping IP pools. After configuring the `vlan-map`, move to the Port Ethernet configuration mode to attach the `vlan-map` to a specific vlan.

**Example**
The following command sets an IPv4 for a next-hop gateway.

```
vlan-map next-hop 123.123.123.1
```
Chapter 206
x-header Format Configuration Mode Commands

The x-header Format Configuration Mode is used to create and configure extension-header (x-header) formats.

**Important:** This feature is license dependent. Please contact your local sales representative for more information.

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

This command returns the CLI prompt to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec mode.
exit

This command exits the current configuration mode and returns the CLI prompt to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to change to the parent configuration mode.
**insert**

This command configures the x-header fields to be inserted in HTTP/WSP GET and POST request packets.

---

**Important:** This command is license dependent. Please contact your local sales representative for more information.

---

**Product**

ECS

**Privilege**

Security Administrator, Administrator

**Syntax**

In StarOS 8.0:

```
insert xheader_field_name { string-constant xheader_field_value | variable { bearer { 3gpp charging-id | ggsn-address | imsi | radius-calling-station-id | sgsn-address | sn-rulebase | subscriber-ip-address } | http { host | url } }
```

```
no insert xheader_field_name
```

In StarOS 8.1, StarOS 9.0 and later releases:

```
insert xheader_field_name { string-constant xheader_field_value | variable { bearer { 3gpp | apn | charging-characteristics | charging-id | imei | imsi | rat-type | sgsn-address | acr | customer-id | ggsn-address | mdn | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | username } [ encrypt ] | http { host | url } }
```

```
no insert xheader_field_name
```

---

**no**

Removes the specified x-header field configuration.

---

**xheader_field_name**

Specifies the x-header field name to be inserted in the packets.

- `xheader_field_name` must be an alpha and/or numeric string of 1 through 31 characters in length.
- Up to 10 fields can be inserted in each x-header format.

---

**string-constant xheader_field_value**

Specifies constant string value for x-header field to be inserted in the packets.

- `xheader_field_value` must be the x-header field value, and must be an alpha and/or numeric string of 1 through 63 characters in length.

---

**variable**

Specifies name of the x-header field whose value must be inserted in the packets.
bearer { 3gpp { apn | charging-characteristics | charging-id | imei | imsi | rat-type | sgsn-address } | acr | customer-id | ggsn-address | mdn | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | username } [ encrypt ]

Specifies value of x-header field to be inserted:

- **3gpp**: 3GPP service
  - **apn**: APN of the bearer flow. This field is deprecated from under `bearer apn` and has been added within `bearer 3gpp apn`
  - **charging-characteristics**: Charging characteristics of the bearer flow
  - **charging-id**: Charging ID of the bearer flow
  - **imei**: IMEI or IMEISV (depending on the case) associated with the bearer flow
  - **imsi**: Specific Mobile Station Identification number.
  - **rat-type**: This field is deprecated from under `bearer rat-type` and has been added within `bearer 3gpp rat-type`
  - **sgsn-address**: SGSN associated with the bearer flow
  - **acr**: Anonymous Customer Reference. Only MSISDN part of this is encrypted, if encrypt flag is set.
  - **customer-id**: Customer ID of the bearer
  - **ggsn-address**: GGSN IP address field
  - **imsi**: This field is deprecated from within `bearer imsi` and has been moved within `bearer 3gpp imsi`
  - **mdn**: MDN of the bearer flow
  - **radius-calling-station-id**: Calling Station ID of the mobile handling the flow
  - **session-id**: Accounting session ID of the bearer flow
  - **sn-rulebase**: Name of the ECS rulebase
  - **sgsn-address**: This field is deprecated from under `bearer sgsn-address` and has been moved within `bearer 3gpp sgsn-address`
  - **subscriber-ip-address**: Subscriber IP address
  - **username**: User name of the bearer flow

**encrypt**: Specifies encryption of x-header field configuration. This option must only be configured in the case of x-header encryption feature.

http { host | url }

Specifies value of the x-header field to be inserted:

- **host**: Host
- **url**: Uniform Resource Locator

**Usage**

Use this command to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets. The x-headers would be inserted at the end of HTTP/WSP header. This CLI command may be used up to 10 times. There is no control over the order of the fields that are to be inserted. Any of the indicated
ruledef variables may be inserted using the variable option, or a static string may be inserted using the string-constant option. Operators may insert x-headers in some HTTP/WSP packets, for which some rules will be configured. The charging-action associated with these rules will contain the list of x-headers to be inserted in the packets.

Example
The following command configures an x-header field named test12 with a constant string value of testing to be inserted in HTTP/WSP GET and POST request packets:

```
insert test12 string-constant testing
```